(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－131923
（P2003－131923A）
(43)公開日　平成15年５月９日(2003.5.9)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｇ０６Ｆ　12/00	５３７	Ｇ０６Ｆ　12/00	５３７Ｚ　５Ｂ０６５
	５１４		５１４Ｅ　５Ｂ０８２
	５４５		５４５Ａ　５Ｋ０３０
3/06	３０４	3/06	３０４Ｈ
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　12/56	Ｈ

審査請求　未請求　請求項の数34　ＯＬ　外国語出願　（全 48 頁）

(21)出願番号　特願2002－114116(P2002－114116)

(22)出願日　平成14年４月17日(2002.4.17)

(31)優先権主張番号　０９／８３９９５２

(32)優先日　平成13年４月19日(2001.4.19)

(33)優先権主張国　米国（ＵＳ）

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　岩見　直子
アメリカ合衆国カリフォルニア州クパティーノ　アパートメント＃6211　プルネリッジアベニュー　19500

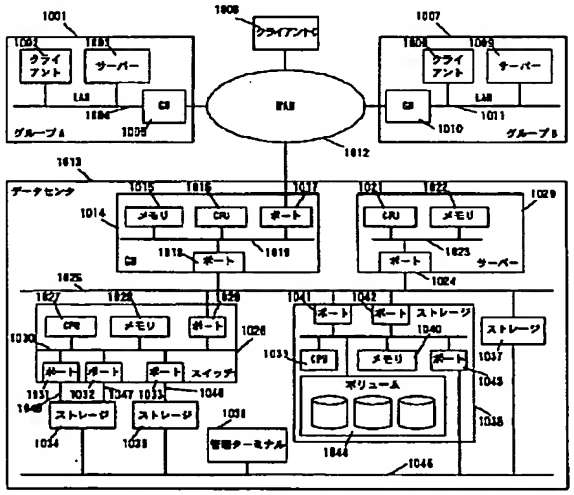
(74)代理人　100075096
弁理士　作田　康夫

Ｆターム(参考)　5B065 BA01 CH04 PA01 PA12
5B082 EA11 FA07 HA00
5K030 GA08 GA15 HA08 HC01 HD03
HD07 KA07

(54)【発明の名称】　仮想プライベートボリューム方式及びシステム

(57)【要約】
【課題】本発明は、ストレージ資源へのアクセスを管理する技術を提供する。
【解決手段】本発明の実施により、ユーザは、仮想アドレスと仮想ボリューム識別子のシステムを用いて、ストレージデバイス内の資源にアクセスできる様になる。本発明の実施により、企業体を含めてユーザが、インターネットまたは他の種類のネットワークを経由して、ユーザのネットワークでSSP（Storage Service Provider)内のボリュームを使用することが可能になる。本発明の実施により、SSPとユーザは、ユーザのデータセンタのみならずSSP内のストレージデバイス、ボリューム、および機器の固有情報を隠蔽し、双方にとってプライバシを確立することができる。

【図１】



【特許請求の範囲】
【請求項１】プロセッサ、メモリ、及び外部ネットワークに接続するための少なくとも１つのポートを持つゲートウエイと、
それぞれが複数のボリュームの少なくとも１つで構成され、情報を記憶する複数のデバイスの少なくとも１台とサーバーと、
スイッチと、
前記ゲートウエイ、前記サーバー、前記スイッチ、及び情報を記憶する前記複数のデバイスの少なくとも１台を接続する内部ネットワークと、で構成されるストレージ装置において、
前記ゲートウエイは、保存のためにデータパケットを受信し、前記メモリを検索して前記データパケットから読み出した仮想受信アドレスを検出し、該仮想受信アドレスに対応して情報を記憶する前記複数のデバイスの少なくとも１台の特定の１台を指定する受信アドレスを前記メモリから読み出し、前記データパケットの前記仮想受信アドレスを前記メモリから読み出した前記対応する受信アドレスに置き換えることを特徴とするストレージ装置。
【請求項２】請求項1記載のストレージ装置において、
前記ゲートウエイは、前記データパケット内のユーザアドレスに基づいて前記データパケットの送信者を認証することを特徴とするストレージ装置。
【請求項３】請求項１記載のストレージ装置において、
前記外部ネットワークは、VPN (Virtual Private Network)で構成され、前記ゲートウエイは前記データパケットに対してVPN処理を実行することを特徴とするストレージ装置。
【請求項４】請求項１記載のストレージ装置において、
前記外部ネットワークは第１のプロトコルを使用し、前記内部ネットワークは第２のプロトコルを使用し、前記ゲートウエイは前記データパケットを前記第１のプロトコルから前記第２のプロトコルに変換することを特徴とするストレージ装置。
【請求項５】請求項4記載のストレージ装置において、
前記第１のプロトコルは、IPプロトコル、ATM、及びファイバチャネルの少なくとも一つから成ることを特徴とするストレージ装置。
【請求項６】請求項４記載のストレージ装置において、
前記第２のプロトコルは、IPプロトコル、ATM、及びファイバチャネルの少なくとも一つから成ることを特徴とするストレージ装置。
【請求項７】請求項７記載のストレージ装置において、
前記ゲートウエイは前記データパケットを検索してコマンドと仮想プライベートボリューム識別子を検出し、検出できたら、前記メモリを検索して前記仮想プライベートボリューム識別子に対応するボリューム識別子を検出し、前記データパケットの前記仮想プライベートボリューム識別子を前記ボリューム識別子で置き換えることを特徴とするストレージ装置。
【請求項８】請求項１記載のストレージ装置装置において、前記ゲートウエイは前記外部ネットワークに送信されるデータパケットを受け取り、前記メモリを検索して前記データパケットから読み出した受信アドレスを検出し、前記メモリから対応する仮想受信アドレスを読み取り、前記データパケットの前記受信アドレスを前記メモリから読み取った前記対応する仮想受信アドレスで置き換えることを特徴とするストレージ装置。
【請求項９】請求項1記載のストレージ装置において、
前記仮想受信アドレスと前記受信アドレスはテーブルに格納されていることを特徴とするストレージ装置。
【請求項１０】プロセッサ、メモリ、及び外部ネットワークに接続するための少なくとも１つのポートより構成されるサーバーと、
情報を記憶し、各々は少なくとも１つのボリュームで構成される少なくとも１台のデバイスと、スイッチと、前記サーバー、前記スイッチ、および情報を記憶する前記複数のデバイスの少なくとも１台を接続する内部ネットワークと、で構成されるストレージ装置において、
前記サーバーはデータパケットを受信してこれを保存し、前記メモリを検索して前記データパケットから読み出した仮想受信アドレスを検出し、前記メモリより前記仮想受信アドレスに対応して前記デバイスの特定の１台を指定する受信アドレスを読み出し、前記データパケットの前記仮想受信アドレスを前記メモリから読み出した前記対応する受信アドレスに置き換えることを特徴とするストレージ装置。
【請求項１１】請求項１０記載のストレージ装置は、さらに、ゲートウエイから構成され、前記ゲートウエイは、プロセッサ、メモリ、及び外部ネットワークに接続するための少なくとも１つのポートを有し、前記外部ネットワークは第１のプロトコルを使用し、前記内部ネットワークは第２のプロトコルを使用し、前記ゲートウエイは前記データパケットを前記第１のプロトコルから前記第２のプロトコルに変換することを特徴とするストレージ装置。
【請求項１２】請求項１１記載のストレージ装置において、前記第１のプロトコルは、IPプロトコル、ATM、及びファイバチャネルの少なくとも一つから成ることを特徴とするストレージ装置。
【請求項１３】請求項１１記載のストレージ装置において、前記第２のプロトコルは、IPプロトコル、ATM、及びファイバチャネルの少なくとも一つから成ることを特徴とするストレージ装置。
【請求項１４】請求項１１記載のストレージ装置において、前記外部ネットワークはVPN (Virtual Private Network)で構成され、前記ゲートウエイは前記データパケ

レージ装置。
【請求項１５】請求項１０記載のストレージ装置において、前記サーバーは前記データパケットを検索してコマンドと仮想プライベートボリューム識別子を検出し、検出できたら、前記メモリを検索して前記仮想プライベートボリューム識別子に対応するボリューム識別子を検出し、前記データパケットの前記仮想プライベートボリューム識別子を前記ボリューム識別子で置き換えることを特徴とするストレージ装置。
【請求項１６】請求項１０記載のストレージ装置において、前記サーバーは前記外部ネットワークに送信されるデータパケットを受け取り、前記メモリを検索して前記データパケットから読み出した受信アドレスを検出し、前記メモリから対応する仮想受信アドレスを読み取り、前記データパケットの前記受信アドレスを前記メモリから読み取った前記対応する仮想受信アドレスで置き換えることを特徴とするストレージ装置。
【請求項１７】請求項１０記載のストレージ装置において、前記サーバーは前記データパケット内のユーザアドレスに基づいて前記データパケットの送信者を認証することを特徴とするストレージ装置。
【請求項１８】プロセッサ、メモリ、及び外部ネットワークに接続するための少なくとも１つのポートより構成されるスイッチと、情報を記憶し各々は複数のボリュームの少なくとも１つで構成される複数のデバイスの少なくとも１台と、サーバーと、前記サーバー、前記スイッチ、および情報を記憶する前記複数のデバイスの少なくとも１台を接続する内部ネットワークと、で構成されるストレージ装置において、
前記スイッチはデータパケットを受信してこれを保存し、前記メモリを検索して前記データパケットから読み出した仮想受信アドレスを検出し、前記メモリから前記仮想受信アドレスに対応して情報を記憶する前記複数のデバイスの少なくとも１台の特定の１台を指定する受信アドレスを読み出し、前記データパケットの前記仮想受信アドレスを前記メモリから読み出した前記対応する受信アドレスに置き換えることを特徴とするストレージ装置。
【請求項１９】請求項１８記載のストレージ装置は、さらに、ゲートウエイから構成され、前記ゲートウエイは、プロセッサ、メモリ、及び外部ネットワークに接続するための少なくとも１つのポートを有し、前記外部ネットワークは第１のプロトコルを使用し、前記内部ネットワークは第２のプロトコルを使用し、前記ゲートウエイは前記データパケットを前記第１のプロトコルから前記第２のプロトコルに変換することを特徴とするストレージ装置。
【請求項２０】請求項１９記載のストレージ装置において、前記第１のプロトコルは、IPプロトコル、ATM、及びファイバチャネルの少なくとも一つから成ることを特徴とするストレージ装置。
【請求項２１】請求項１９記載のストレージ装置において、前記第２のプロトコルは、IPプロトコル、ATM、及びファイバチャネルの少なくとも一つから成ることを特徴とするストレージ装置。
【請求項２２】請求項１９記載のストレージ装置において、前記外部ネットワークはVPN (Virtual Private Network)で構成され、前記ゲートウエイは前記データパケットに対してVPN処理を実行することを特徴とするストレージ装置。
【請求項２３】請求項１８記載のストレージ装置において、前記スイッチは前記データパケットを検索してコマンドと仮想プライベートボリューム識別子を検出し、検出できたら、前記メモリを検索して前記仮想プライベートボリューム識別子に対応するボリューム識別子を検出し、前記データパケットの前記仮想プライベートボリューム識別子を前記ボリューム識別子で置き換えることを特徴とするストレージ装置。
【請求項２４】請求項１８記載のストレージ装置において、前記スイッチは前記外部ネットワークに送信されるデータパケットを受け取り、前記メモリを検索して前記データパケットから読み出した受信アドレスを検出し、前記メモリから対応する仮想受信アドレスを読み取り、前記データパケットの前記受信アドレスを前記メモリから読み取った前記対応する仮想受信アドレスで置き換えることを特徴とするストレージ装置。
【請求項２５】請求項１８記載のストレージ装置において、前記スイッチは前記データパケット内のユーザアドレスに基づいて前記データパケットの送信者を認証することを特徴とするストレージ装置。
【請求項２６】情報を記憶し、各々は複数ボリュームの少なくとも１つ、プロセッサ、メモリ、及び外部ネットワークに接続するための少なくとも１つのポートから構成される複数のデバイスの少なくとも１台と、スイッチと、サーバーと、前記サーバー、前記スイッチ、および前記情報を記憶する複数デバイスの少なくとも１台を接続する内部ネットワークと、で構成されるストレージ装置において、
前記情報を記憶する複数のデバイスの少なくとも１台はデータパケットを受信してこれを保存し、前記メモリを検索して前記データパケットから読み出した仮想受信アドレスを検出し、前記メモリから前記仮想受信アドレスに対応して前記情報を記憶する複数のデバイスの少なくとも１台の特定の１台を指定する受信アドレスを読み出し、前記データパケットの前記仮想受信アドレスを前記メモリから読み出した前記対応する受信アドレスに置き換えることを特徴とするストレージ装置。
【請求項２７】請求項２６記載のストレージ装置は、さらに、ゲートウエイから構成され、前記ゲートウエイは、プロセッサ、メモリ、及び外部ネットワークに接続

するための少なくとも１つのポートを有し、前記外部ネットワークは第１のプロトコルを使用し、前記内部ネットワークは第２のプロトコルを使用し、前記ゲートウエイは前記データパケットを前記第１のプロトコルから前記第２のプロトコルに変換することを特徴とするストレージ装置。

【請求項２８】請求項２７記載のストレージ装置において、前記第１のプロトコルは、IPプロトコル、ATM、及びファイバチャネルの少なくとも一つから成ることを特徴とするストレージ装置。

【請求項２９】請求項２７記載のストレージ装置において、前記第２のプロトコルは、IPプロトコル、ATM、及びファイバチャネルの少なくとも一つから成ることを特徴とするストレージ装置。

【請求項３０】請求項２７記載のストレージ装置において、前記外部ネットワークはVPN（Virtual Private Network）で構成され、前記ゲートウエイは前記データパケットに対してVPN処理を実行することを特徴とするストレージ装置。

【請求項３１】請求項２６記載のストレージ装置において、前記情報を記憶する複数のデバイスの少なくとも１台は、前記データパケットを検索してコマンドと仮想プライベートボリューム識別子を検出し、検出できたら、前記メモリを検索して前記仮想プライベートボリューム識別子に対応するボリューム識別子を検出し、前記データパケットの前記仮想プライベートボリューム識別子を前記ボリューム識別子で置き換えることを特徴とするストレージ装置。

【請求項３２】請求項２６記載のストレージ装置において、前記情報を記憶する複数のデバイスの少なくとも１台は、前記外部ネットワークに送信されるデータパケットを受け取り、前記メモリを検索して前記データパケットから読み出した受信アドレスを検出し、前記メモリから対応する仮想受信アドレスを読み取り、前記データパケットの前記受信アドレスを前記メモリから読み出した前記対応する仮想受信アドレスで置き換えることを特徴とするストレージ装置。

【請求項３３】請求項２６記載のストレージ装置において、前記情報を記憶する複数のデバイスの少なくとも１台は、前記データパケット内のユーザアドレスに基づいて前記データパケットの送信者を認証することを特徴とするストレージ装置。

【請求項３４】ストレージを管理する方法であって、前記方法は、

データパケットを受信し、

前記データパケットから抽出した仮想受信アドレスを検索し、

前記仮想受信アドレスに対応し、情報を記憶する複数のデバイスの少なくとも１台の特定の１台を指定する受信アドレスを読み出し

前記データパケットの前記仮想受信アドレスを前記対応する受信アドレスで置き換えることから構成されることを特徴とする方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、一般的にデータストレージシステムに関連し、特に、仮想ボリュームを用いてストレージアクセスを制御する技術に関連する。

【０００２】

【従来の技術】情報技術の発展とともに、ビジネス企業体は益々増大するストレージ容量が必要になっている。平均的フォーチュン１０００企業においては、来るべき年には、倍以上のストレージ容量が必要になると予想されている。加えて、容量の増大は熟練した情報技術者の不足をもたらしている。このため、多くの企業は、情報技術への投資の拡大を余儀なくさせられている。

【０００３】容量の急激な増大要求に対抗するため、ストレージ管理を次第に外部委託する企業が増加している。SSP（Storage Service Provider）は、ビジネス企業体に提供できるストレージ管理サービスのひとつになっている。SSPに委ねることにより、企業体はSSPサービス提供者より必要に応じてストレージ資源を得ることが出来る。

【０００４】SSPはストレージ管理サービスを提供するのみならず、ストレージシステムを自ら所有して、ユーザのホストシステムが使用するためのストレージ容量をも提供する。ユーザはSSPとの間のSLA（Service Level Agreement）契約に従って、ストレージ使用と管理サービスの為の支払いをする。

【０００５】

【発明が解決しようとする課題】現在のSSP技術により、そこそこの便益は期待できるものの、更なる改良の余地が存在する。例えば、現状の慣用的なSSP技術によれば、SSPは、SSPサイトでSSPが所有しているデイスクストレージシステムのストレージ資源を、ユーザサイトのホストシステムの為に提供する。

【０００６】しかしながら、SSPユーザによっては、自らの装置をSSPサイトより遠隔地に設置する事を望むかもしれない。例えば、ユーザはSSP内のストレージシステムに保持されているデータを、インターネットまたは他のネットワークを通してアクセスしてもよい。さらに、セキュリテイが、ユーザ及びSSP双方にとって重要な懸案事項である。ユーザにとっては、この事は、貴重なビジネス情報資産がストレージ内のデータに対するアクセスを制限することにより守られることを意味する。

【０００７】SSPにとっては、この事は、データの正当性が各顧客に対して保証され、ユーザが認証されないアクセスを受けることはない、ということを意味する。例えば、大会社の各部門では、他の部門からアクセスされない自部門専用のストレージ資源を持ちたいこともあり

得る。真に要求される技術は、ストレージ資源へのアクセスを管理するための改良された技術である。

【０００８】

【課題を解決するための手段】本発明は、ストレージ資源へのアクセスを管理する技術を提供する。本発明の実施により、ユーザは仮想アドレスと仮想ボリューム識別子のシステムを用いてストレージデバイス内の資源にアクセスできる様になる。本発明の実施により、たとえば企業体を含めてユーザが、インターネットまたは他の種類のネットワーク接続を経由して、ユーザのネットワークでSSP (Storage Service Provider)内のボリュームを使用することが可能になる。

【０００９】本発明の実施により、SSPとユーザは、ユーザのデータセンタのみならずSSP内のストレージデバイス、ボリューム、および機器の固有情報を隠蔽し、双方にとってプライバシを確立することができる。

【００１０】本発明の代表的な実施では、ストレージ装置が提供される。本ストレージ装置は、プロセッサ、メモリ、外部ネットワークに接続するための少なくとも１つのポートを持つゲートウエイと、情報を記憶し各々１つ以上のボリュームから構成される１台以上のデバイス、サーバー、スイッチ、及び該ゲートウエイ、該サーバー、該スイッチ、および該情報を記憶する１台以上のデバイスを接続する内部ネットワークで構成される。

【００１１】ゲートウエイはデータパケットを受信しこれを記憶し、メモリを検索して該データパケットより抽出した仮想受信アドレスを検出し、該仮想受信アドレスに対応し情報を記憶する1台以上のデバイスの特定の１台を指定する受信アドレスをメモリより読み出し、該データパケットの該仮想受信アドレスをメモリから読み出した対応する受信アドレスで置き換える。

【００１２】実施例では、仮想受信アドレスと受信アドレスは、テーブルに格納されている。しかしながら、別の実施例としては、これらのアドレスは、ボリューム識別子、ユーザ識別子と共に、他のタイプのデータ構造、例えば、リンクリスト、キュー、スタック等に格納されても良い。さらに、このようなデータ構造は、メモリに配置されても、デイスクストレージなどに格納されても良い。

【００１３】実施例によっては、ゲートウエイは、データパケット内のユーザアドレスに基づいてデータパケットの発信源の認証を行う。ある実施例では、外部ネットワークは、VPN (Virtual Private Network)機能を有する。このような実施例においては、例えば、ゲートウエイがデータパケットに対するVPN処理を実行する。

【００１４】実施例によっては、外部ネットワークは第１のプロトコルを使用し、内部ネットワークは第１のプロトコルとは異なる第２のプロトコルを使用する。このような場合は、例えば、ゲートウエイが、データパケットを第１のプロトコルから第２のプロトコルに変換する。第１のプロトコルは、たとえばIPプロトコル、ATM、及びファイバチャネルのどれでも、または本分野の技術者であれば公知の他のタイプのプロトコルでも構わない。同様に、第２のプロトコルは、上記のプロトコルのどれかである。

【００１５】実施例によっては、ゲートウエイは、データパケットを検索してコマンドと仮想プライベートボリューム識別子を検出し、検出されれば、メモリを検索して該仮想プライベートボリューム識別子に対応するボリューム識別子を見つけて、該データパケット内の該仮想プライベートボリューム識別子を該ボリューム識別子で置き換える。

【００１６】実施例によっては、ゲートウエイは、外部ネットワークに送信されるデータパケットを受け取り、メモリを検索して該データパケットより抽出された受信アドレスを検出し、メモリから対応する仮想受信アドレスを読み込み、該データパケット内の該受信アドレスをメモリから読み込んだ対応する仮想受信アドレスで置き換える。

【００１７】本発明の他の実施例では、ストレージ装置が提供される。本ストレージ装置は、プロセッサ、メモリ、および外部ネットワークに接続するための少なくとも１つのポートを持つサーバー、情報を記憶し各々が１つ以上のボリュームで構成される１台以上のデバイス、スイッチ、及び該サーバー、該スイッチ、該情報を記憶する１台以上のデバイスを接続する内部ネットワークで構成される。

【００１８】該サーバーは、データパケットを受信しこれを記憶し、メモリを検索して該データパケットより抽出した仮想受信アドレスを検出し、該仮想受信アドレスに対応し情報を記憶する１台以上のデバイスの特定の１台を指定する受信アドレスをメモリから読み込み、該データパケットの該仮想受信アドレスをメモリから読み込んだ対応する受信アドレスで置き換える。

【００１９】本発明の他の実施例では、ストレージ装置が提供される。本ストレージ装置は、プロセッサ、メモリ、および外部ネットワークに接続するための少なくとも１つのポートを持つスイッチと、情報を記憶し各々が１つ以上のボリュームで構成される１台以上のデバイス、サーバー、及び該サーバー、該スイッチ、該情報を記憶する１台以上のデバイスを接続する内部ネットワークで構成される。

【００２０】該スイッチは、データパケットを受信しこれを記憶し、メモリを検索して該データパケットより抽出した仮想受信アドレスを検出し、該仮想受信アドレスに対応し情報を記憶する１台以上のデバイスの特定の１台を指定する受信アドレスをメモリから読み込み、該データパケットの該仮想受信アドレスをメモリから読み込んだ対応する受信アドレスで置き換える。

【００２１】本発明の他の実施例では、ストレージ装置

が提供される。本ストレージ装置は、情報を記憶し各々が１つ以上のボリューム、プロセッサ、メモリ、および外部ネットワークに接続するための少なくとも１つのポートから構成される１台以上のデバイス、スイッチ、サーバー、及び該サーバー、該スイッチ、および該情報を記憶する１台以上のデバイスを接続する内部ネットワークで構成される。

【００２２】該情報を記憶する１台以上のデバイスは、データパケットを受信しこれを記憶し、メモリを検索して該データパケットより抽出した仮想受信アドレスを検出し、該仮想受信アドレスに対応し情報を記憶する１台以上のデバイスの特定の１台を指定する受信アドレスをメモリから読み出し、該データパケットの該仮想受信アドレスをメモリから読み出した対応する受信アドレスで置き換える。

【００２３】本発明の代表的な実施例では、ストレージを管理する方法が提供される。本方法は、データパケットを受信し、該データパケットより仮想受信アドレスを抽出し、該仮想受信アドレスに対応する情報を記憶する１台以上のデバイスの特定の１台を指定する受信アドレスをメモリから読み出し、該データパケットの該仮想受信アドレスを該対応する受信アドレスで置き換えることを含む。

【００２４】本発明により、慣用的技術に勝る数々の便益が実現される。本発明の実施により、企業体を含めてユーザが、インターネット、または他の種類のネットワーク接続を経由して、ユーザのネットワークで、SSP (Storage Service Provider)内のボリュームを使用することが可能になる。

【００２５】本発明の実施により、SSPとユーザは、ユーザのデータセンタのみならずSSP内のストレージデバイス、ボリューム、および機器の固有情報を隠蔽し、双方にとってプライバシを確立することができる。各種の便益が本明細書で述べられている。本発明の更なる本質と便益は、本明細書のこれからの部分と添付図面を参照することにより、明らかになる。

【００２６】

【発明の実施の形態】本発明は、ストレージ資源へのアクセスを管理する技術を提供するものである。本発明により、ユーザは、ストレージデバイスの仮想アドレスと仮想ボリューム識別子(ID)のシステムを用いてストレージ資源へアクセス出来るようになる。本発明の実施により、SSP (Storage Service Provider)は、インターネットまたは他の種類のネットワーク接続を通して、例えば企業体も含めて、ユーザのネットワークでユーザに対してボリュームを利用可能にする。

【００２７】本発明の実施により、SSPとユーザは、ユーザのデータセンタのみならずSSP内のストレージデバイス、ボリューム、及び装置の固有情報を隠蔽し、双方に[illegible]

al Private Network)は、インターネットのようなパブリックネットワークを用いて、プライベートネットワーク環境を実現する為のネットワーク技術である。

【００２８】VPNを使用して、２つ以上のネットワークがインターネットを通して接続でき、１つのプライベートネットワークとして互いに交信できるようになる。現状の慣用的VPN技術の注目すべき限界の１つは、VPNを構成するネットワーク機器のすべての固有情報を隠蔽するものではないことである。

【００２９】ゾーン技術は、FC (Fibre Channel)スイッチで採用されている技術である。ゾーン技術では、１つのポートを他のポートに割り当て可能にし、１つのポートに接続されている装置が、自ポートに割り当てられるべき他のポートに接続されているボリュームを使用出来るようにする。通常は、各装置は直接FCスイッチに接続される。

【００３０】さらに、慣用的なゾーン技術では、共通のポートに接続され、他の装置から使用されてしまう可能性があるボリュームの固有情報を隠蔽しない。LUN (LogicalUnit Number)セキュリテイは、例えば、ファイバチャネルで接続されたストレージデバイスがWWN (World Wide Names)と呼ばれる装置の固有情報を検出し、ストレージデバイス内のボリュームの固有情報を不当アクセスから保護するストレージ技術である。通常は、各装置は直接FCスイッチに接続される。さらに、慣用的な手法では、ユーザはLUNとポートアドレスを認識するだろう。

【００３１】図１は、本発明の一実施例でのSSP (Storage Service Provider)の代表的な構成を示す図である。グループA１００１は、ユーザのローカルネットワークを示している。グループB１００７は、もう一つのユーザのローカルネットワークを示している。クライアントC１００６は、個人ユーザを示している。データセンタ１０１３は、実施例では、SSPに相当するストレージプロバイダの装置で構成される。データセンタ１０１３は、少なくとも１つのゲートウエイ１０１４と少なくとも１つのストレージ１０３８を有する。

【００３２】ユーザはWAN (Wide Area Network)１０１２を通して、データセンタ１０１３に接続できる。WAN１０１２は、例えば、インターネットやATMリース回線などである。各ユーザは、例えば、同じネットワークを使用してデータセンタ１０１３に接続できる。ユーザは、専用のリース回線を使用してデータセンタ１０１３に直接接続することもできる。ゲートウエイ１０１４は、データセンタ１０１３外のネットワーク１０１２に接続する為の少なくとも１つのポート１０１７を有する。

【００３３】ゲートウエイ１０１４は、データセンタ１０１３内のネットワーク１０２５に接続する為の少なくとも１つのポート１０１８を有する。ネットワーク１０[illegible]

れる。ストレージ１０３８はネットワーク１０２５と接続する為の少なくとも１つのポート１０４２を有する。ボリューム１０４４はストレージ１０３８に対して定義され、例えば、SCSI (Small Computer System Interface)プロトコルで定義されるLUN (Logical UnitNumber)として使用されるボリュームIDを持つ。

【００３４】ポート１０４３はネットワーク１０４５に接続され、管理の為に使用される。管理ターミナル１０３６はストレージ１０３８、１０３７、１０３４、１０３５にネットワーク１０４５経由で接続され、ストレージ構成を定義する為に使用される。スイッチ１０２６はネットワーク１０２５に接続する為の少なくとも１つのポート１０２９を有する。スイッチ１０２６はストレージ１０３４に接続する為の少なくとも１つのポート１０３１を有する。他の実施例、例えば、ネットワーク１０２５とネットワーク１０４５が共にIPネットワークの様に同じタイプの場合は、両ネットワークは１つのネットワークとして統合されても良い。

【００３５】他の実施例、例えば、ネットワーク１０１２がネットワーク１０２５と異なるネットワーク、例えば、ネットワーク１０１２がIPネットワークで、ネットワーク１０２５がFCネットワークの場合は、ゲートウエイ１０１４がこの異なるネットワーク間のプロトコル変換の役割を果たす。ストレージ１０３４が、例えば、ネットワーク１０２５がIPネットワークで、ネットワーク１０４８がFCネットワークのように異なったタイプのネットワークをサポートする実施例の場合は、スイッチ１０２６が両者間のプロトコル変換の役割を果たす。

【００３６】このような実施例の場合は、ストレージ１０３４とストレージ１０３８は異なったネットワークプロトコルをサポートする。例えば、ネットワーク１０４８とネットワーク１０４６が異なったプロトコルをサポートし、ネットワーク１０４６がネットワーク１０２５と同じプロトコルを採用する場合は、スイッチ１０２６がプロトコル変換の役割を果たす。さらに、 ストレージ１０３４とストレージ１０３８は異なったネットワークプロトコルをサポートし、異なったストレージアクセスプロトコルを採用する事もできる。

【００３７】もう一つの実施例として、ネットワーク１０４８とネットワーク１０４６が異なったネットワークプロトコルを採用し、ストレージ１０３４とストレージ１０３５がスイッチ１０２６を通して交信する場合は、スイッチ１０２６がプロトコル変換の役割を果たす。さらに、ストレージ１０３４とストレージ１０３８は異なったネットワークプロトコルをサポートし、異なったストレージアクセスプロトコルを採用する事もある。データセンタ１０１３はスイッチ１０２６、または、サーバー１０２０、または双方が省略されても良い。

【００３８】図２は本発明の一実施例での代表的なプロ

例で示されるプログラムは、図１のゲートウエイ１０１４のメモリ１０１５中に展開される。図２の実施例で示されるように、通信プログラム２００１は、１つ以上のVPN (Virtual Private Network) プログラム２００２、認証プログラム２００３、ビュープログラム２００４、プロトコル変換プログラム２００５、及び送受信プログラム２００６を含む複数の要素プログラムプロセスで構成される。

【００３９】VPN プログラム２００２は、ユーザがパブリックネットワークを使用してデータセンタ１０１３内のボリュームにアクセスするのにプライベートネットワークを定義できる様にする。ユーザが、パブリックネットワークを使用してプライベートネットワークを定義するためのVPNを使用しない場合は、VPN プログラム２００２は省略可能である。認証プログラム２００３は、データセンタ１０１３内のストレージデバイス１０３４内の情報にアクセスしようとしているユーザの認証を可能とする。

【００４０】ゲートウエイ１０１４がユーザ認証を行わない場合は、認証プログラム２００３は省略可能である。ビュープログラム２００４は、データセンタ１０１３内のデータ蓄積用ボリュームに対する仮想及び実アドレスの変換を実行する。プロトコル変換プログラム２００５は、例えば、IPネットワークとFCネットワークの如く、異なったトポロジのネットワークで結合された装置が互いに交信できる様に、プロトコル変換を行う。

【００４１】さらに、プロトコル変換プログラム２００５は、例えば、SCSIとFCの如く、異なったストレージアクセスプロトコルを持つ装置が互いに交信できる様にもする。データセンタ１０１３外のネットワーク１０１２とデータセンタ１０１３内のネットワーク１０２５が同じ種類の場合は、プロトコル変換プログラム２００５は省略可能である。送受信プログラム２００６はネットワークを経由した通信を司る。ビューテーブル２００７は、ビュープログラム２００４が利用できる様に、多様なユーザに割り当てられたデータセンタ１０１３内のストレージに関する情報を維持しており、メモリ１０１５内に展開される。

【００４２】図３は、本発明の一実施例でのビューテーブルの代表的なフォーマットを示す図である。図３の実施例に示される如く、ビューテーブル２００７はユーザ用の複数の情報欄により構成される。ユーザタイプ３００１はユーザに関する情報を示す。ユーザアドレス３００２は、個別ユーザのマシンのアドレス、または、複数ユーザのアドレスグループを示す。例えば、ユーザグループ３００７のように、ユーザタイプ３００１が”グループ”にセットされている場合は、グループ３００７に属するユーザは、データセンタ１０１３内の同一ボリュームにアクセスする共通ユーザセットのアドレス３０１

【００４３】ユーザタイプ３００１が３００８の如く、"個人"にセットされている場合は、ユーザは、データセンタ１０１３内のボリュームにアクセスできるユーザアドレス３０１１で定義される。仮想受信アドレスVDA (Virtual Destination Address) ３００３は、ユーザに開示されているストレージユニットを指定する為にユーザが使用するアドレスである。

【００４４】ストレージデバイスは、ユーザの情報が蓄積され、ユーザに開示されているボリュームを持つ。ユーザがデータセンタ１０１３をアクセスするのにVPNを使用する実施例においては、VDAはVPNを使用するユーザによって定義されたプライベートネットワークでのIPアドレスである。受信アドレス３００４は、データセンタ１０１３内のストレージデバイスのアドレスで、ユーザには開示されていない。例えば、受信アドレス３００４は、IPアドレス、ホスト名、ファイバチャネルのWWN (World Wide Name)等である。

【００４５】ストレージユニットがネットワーク接続の為に２つ以上のポートを持っている場合は、各ポート毎に受信アドレス３００４が定義される。仮想プライベートボリュームID３００５は、ユーザがアクセスしたいボリュームを指定する為にユーザによって使用されるアドレスである。ボリュームID３００６は、ユーザには開示されていないボリュームIDである。ボリュームID３００６は、例えば、多くの実装例では、SCSIプロトコルで定義されるLUN (Logical Unit Number)で良い。ストレージユニットは、ボリュームID３００６を用いてボリュームにアクセスする。

【００４６】図４は、本発明の一実施例での代表的な通信プログラムを示すフローチャートである。図２に示される如く、本実施例では、通信プログラム２００１はゲートウエイ１０１４内のメモリ１０１５に存在する。通信プログラム２００１は、データセンタ１０１３内のボリュームのひとつに格納すべきデータを含んだデータパケットを受信し処理する。

【００４７】データパケットを受信後、ステップ４００１にて、パケットは、例えば、グループAのクライアント１００２の様な、データセンタの外部から受信した内向きデータパケットか否かが判定される。データパケットがデータセンタ１０１３の外部から受信された場合は、処理はステップ４００２に進み、そうでなければステップ４００８に進む。データセンタ１０１３との接続にVPNを使用する場合は、オプションステップ４００２にて、パケットはVPNプログラム２００２によって処理される。

【００４８】実施例によっては、VPNを使用する場合は、パブリックネットワークでデータを送信する前にデータを暗号化し、受信後に復号処理を行う。セキュリティをより確実にする為、データのみならず送受信のネット

がって、VPNプログラム２００２はデータパケットのデータに加えて追加的にアドレス情報についても復号処理を実施する。

【００４９】次に、オプションステップ４００３にて、認証プログラム２００３によりパケットの認証確認がなされる。パケットが認証されると、処理はステップ４００４に進み、そうでなければ、ステップ４００７にてパケットは拒絶される。オプションステップ４００４にて、プロトコル変換プログラム２００５が、必要なプロトコル変換をすべて実施する。例えば、データパケットフォーマット、アドレスフォーマット等が変換される。

【００５０】次に、ステップ４００５にて、ビュープログラム２００５が、ビューテーブル２００７の当該パケット発信者のエントリにしたがって、データパケット内のアドレスとボリューム情報の変換を行う。内向きパケットの場合は、仮想受信アドレスを受信アドレスに、仮想ボリュームIDをボリュームIDに置き換える。

【００５１】本実施例での代表的なビュープログラムの処理例を図５に示す。ステップ４０１５にて、ビュープログラム２００５の処理結果がチェックされる。ビュープログラムが"no good (NG)"を返した場合は、パケットはステップ４００７にて拒絶され、次のパケット処理の為にステップ４００１に戻る。

【００５２】逆に、ビュープログラムが"no good (NG)"を返さなかった場合は、ステップ４００６にて、パケットはデータセンタ内のネットワーク１０２５に送られ、処理は次のパケット処理の為にステップ４００１に戻る。

【００５３】データパケットがデータセンタ１０１３の外部から受信されたものではなかった場合は、ステップ４００８にて、当該データパケットはデータセンタ１０１３の内部より外部に発信された外向きパケットか否かが判定される。当該パケットがデータセンタ１０１３の内部、例えばストレージ１０３８、から受信されたものなら、ステップ４００９にて、ビュープログラム２００５がビューテーブル２００７内の当該データパケット発信者のエントリにしたがって、データパケット内のアドレスとボリューム情報の変換を行う。

【００５４】外向きパケットの場合は、受信アドレスを仮想受信アドレスに、ボリュームIDを仮想ボリュームIDに置き換える。そうでない場合は、ステップ４０１３にて、処理を終了して良いか、または、ステップ４０１４にてエラー回復処理を行ってから次のパケット処理の為にステップ４００１に戻るか、を判定する。次に、必要ならオプションステップ４０１０にて、データパケットのプロトコル変換が実施される。

【００５５】次に、VPN使用時には、オプションステップ４０１１にて、VPNプログラム２００２がデータパケット処理を行う。VPNプログラム２００２は、データパ

報についても暗号化処理を実施する。次に、ステップ４０１２にて、当該データパケットはデータセンタ１０１３の外部ネットワーク１０１２に送信される。VPNがサポートされていない、または使用されない実施例では、VPN処理ステップ４００２と４０１１は省略される。

【００５６】データセンタ１０１３の外部のネットワーク１０１２とデータセンタ１０１３の内部のネットワーク１０２５が同じタイプの場合、プロトコル変換処理ステップ４００４と４０１０は省略可能である。ゲートウエイがユーザチェックを行わない場合は、認証処理ステップ４００３は省略可能である。

【００５７】図５は、本発明の一実施例での代表的なビュープログラム処理を示すフローチャートである。本実施例の図５で示されるビュープログラム処理は、図２のビュープログラム２００４と図４のステップ４００５と４００９の処理に対応する。実施例では、データパケット受信後、ステップ５００１にて、当該データパケットはデータセンタ１０１３の外部から受信された内向きデータパケットか否かが判定される。

【００５８】当該データパケットがデータセンタ１０１３の外部からのものであれば、ステップ５０１２にて、ユーザによって定義され、ユーザによって使用されるストレージアドレスである仮想受信アドレス３００３はユーザにとって正しいか否かが判定される。本チェックは、各ユーザの正しいアドレスを登録しているビューテーブル２００７を参照することにより実施される。

【００５９】実施例では、仮想受信アドレス３００３は、当該データパケットを送信したユーザに対して正しいアドレスか否かがチェックされる。仮想受信アドレス３００３が正しくなければ、処理は、"no good (NG)"応答を呼び出したプロセスに返す。正しい場合は、ステップ５００２にて、図３のビューテーブル２００７を検索して当該データパケット内の仮想受信アドレス３００３に対応する受信アドレス３００４を求める。

【００６０】次に、ステップ５００３にて、当該データパケット内の仮想受信アドレス３００３をビューテーブル２００７から求めた受信アドレス３００４に置き換える。次に、ステップ５００４にて、当該データパケットはストレージアクセスコマンドを含むか否か、また含むなら仮想ボリュームID３００５を含むかが判定される。当該データパケットが仮想ボリュームIDを含まなければ、当該データパケットにおいて仮想受信アドレス３００３を受信アドレス３００４に変換した状態で、OK状態の応答を呼び出したプロセスに返す。

【００６１】仮想ボリュームIDを含めば、ステップ５０１３にて、再度ビューテーブル２００７をチェックして、仮想プライベートボリュームIDがデータパケットを送信したユーザに対して正しいか否かが判定される。仮想プライベートボリュームIDが正しくなければ、処理は"no good (NG)"応答を呼び出したプロセスに返す。正しい場合は、ステップ５００５にて、ビューテーブル２００７を検索して、当該データパケットを送信したユーザに対する仮想プライベートボリュームID３００５を求める。次に、ステップ５００６にて、当該データパケット内の仮想プライベートボリュームID３００５をビューテーブル２００７から求めたボリュームID３００６に置き換える。

【００６２】データパケットがデータセンタ１０１３の外部から受信したのでなければ、本パケットは外向きパケットである。したがって、ステップ５００７にて、ビューテーブル２００７を検索して当該データパケットの受信ユーザに対応する仮想受信アドレス３００３を求める。

【００６３】次に、ステップ５００８にて、当該データパケット内の受信アドレス３００４をビューテーブル２００７より抽出したユーザ用の仮想受信アドレス３００３に置き換える。次に、判定のステップ５００９にて、当該データパケットはストレージアクセスコマンドとボリュームID３００６を含むかが判定される。当該データパケットがストレージアクセスコマンドを含み、当該コマンドがボリュームID３００６を含むなら、ステップ５０１０にて、ビューテーブル２００７を検索して当該ユーザのボリュームID３００６を求める。ステップ５０１１にて、ボリュームID３００６をビューテーブル２００７より抽出したユーザ用の対応する仮想ボリュームID３００５に置き換える。

【００６４】当該データパケットがストレージアクセスコマンドとボリュームIDを含まなければ、ユーザに対する受信アドレスを仮想受信アドレスに変換した状態で、OK状態の応答を呼び出したプロセスに返す。ゲートウエイ１０１４がボリュームIDを扱わない場合は、ステップ５００４、５００５、５００６、５００９、５０１０、５０１１、及び５０１３は省略可能である。

【００６５】図６は、本発明の一実施例でのユーザに見える代表的なストレージシステムの図である。図６に示すように、データセンタ１０１３は情報を記憶するための複数のボリュームを有する。例えば、これらのボリュームは、１０３４、１０３７、１０３８等の複数のストレージユニットより割り当てる事が出きる。複数のユーザは、１つ以上のネットワーク１０１２を使用してデータセンタ１０１３に接続することにより、データセンタ１０１３内の多様なボリューム上の情報にアクセスする。

【００６６】例えば、グループA １００１のユーザは、仮想受信アドレス６００１を用いて、WAN１０１２を通して、データセンタ１０１３に接続する。グループA １００１には、彼らのストレージは仮想ボリューム６００２のイメージとして表われる。グループB １００７の他のユーザは、仮想受信アドレス６００５を用いて、WAN

【００６７】同様に、グループB １００７には、彼らのストレージは、仮想ボリューム６００６のイメージとして表われる。個人ユーザのクライアントC １００６は、仮想受信アドレス６００３を用いて、WAN１０１２を通して、データセンタ１０１３に接続する。ユーザC １００６には、彼らのストレージは仮想ボリューム６００４のイメージとして表われる。

【００６８】したがって、データセンタ１０１３は、各ユーザに対して独立の個別のボリュームがある様に見える。さらに、各ユーザは、データセンタ１０１３内の他のユーザのストレージボリュームを見ることは出来ない。

【００６９】図７は、本発明の一実施例での代表的なプログラムのブロックダイアグラムである。図７の実施例では、プログラムは、図１のサーバー１０２０内のメモリ１０２２内に展開される。図７の実施例で示されるように、通信プログラム２００１は、１つ以上のVPN (Virtual Private Network) プログラム２００２、認証プログラム２００３、ビュープログラム２００４、プロトコル変換プログラム２００５、及び送受信プログラム２００６を含む複数の要素プログラムプロセスで構成される。VPN プログラム２００２は、ユーザがパブリックネットワークを使用してデータセンタ１０１３内のボリュームにアクセスするのにプライベートネットワークを定義できる様にする。

【００７０】ユーザが、パブリックネットワークを使用してプライベートネットワークを定義するためのVPNを使用しない実施例では、VPN プログラム２００２は省略可能である。認証プログラム２００３は、データセンタ１０１３内のストレージデバイス１０３４内の情報にアクセスしようとしているユーザの認証を可能とする。サーバー１０２０がユーザ認証を行わない場合は、認証プログラム２００３は省略可能である。ビュープログラム２００４は、データセンタ１０１３内のデータ蓄積用ボリュームの仮想及び実アドレスの変換を実行する。

【００７１】プロトコル変換プログラム２００５は、例えば、SCSIとFCの様に、異なったストレージアクセスプロトコルを持つ装置が互いに交信できる様にするプロトコル変換機能を有する。ユーザ装置とデータセンタ１０１３内のストレージ装置が、同じ種類のストレージアクセスプロトコルを持つ場合は、プロトコル変換プログラム２００５は、省略可能である。

【００７２】たとえば、ネットワーク１０１２がIPネットワークプロトコルで、ネットワーク１０２５がFCネットワークの様に、異なったネットワークプロトコルを使用している場合は、ゲートウエイ１０１４が異なったタイプのネットワークプロトコル間のプロトコル変換を行う。実施例では、データは、データセンタ１０１３の外部からゲートウエイ１０１４を経由して受信され、ゲー[illegible]

信される。

【００７３】送受信プログラム２００６は、ネットワークを経由した通信機能を提供する。ビューテーブル２００７は、ビュープログラム２００４が利用できる様に、多様なユーザに割り当てられたデータセンタ１０１３内のストレージに関する情報を維持しており、サーバー１０２０内のメモリ１０２２に展開される。図７に示した実施例では、ユーザは、図６に示される様なデータセンタストレージの代表的なユーザイメージを持つことが出来る。

【００７４】図８は、本発明の一実施例での代表的なプログラムのブロックダイアグラムである。図８の実施例では、プログラムは、図１のスイッチ１０２６内のメモリ１０２８に展開される。図８の実施例で示されるように、通信プログラム２００１は、１つ以上のVPN (Virtual Private Network) プログラム２００２、認証プログラム２００３、ビュープログラム２００４、プロトコル変換プログラム２００５、及び送受信プログラム２００６を含む複数の要素プログラムプロセスで構成される。

【００７５】VPN プログラム２００２は、ユーザがパブリックネットワークを使用してデータセンタ１０１３内のボリュームにアクセスするのにプライベートネットワークを定義できる様にする。ユーザが、パブリックネットワークを使用してプライベートネットワークを定義するためのVPNを使用しない実施例では、VPN プログラム２００２は省略可能である。認証プログラム２００３は、データセンタ１０１３内のストレージデバイス１０３４内の情報にアクセスしようとしているユーザの認証を可能とする。

【００７６】スイッチ１０２６がユーザ認証を行わない場合は、認証プログラム２００３は省略可能である。ビュープログラム２００４は、データセンタ１０１３内のデータ蓄積用ボリュームの仮想及び実アドレスの変換を実行する。プロトコル変換プログラム２００５は、例えば、IPネットワークとFCネットワークの様に、異なったトポロジのネットワークで接続された装置が互いに交信できる様にするプロトコル変換機能を実行する。

【００７７】さらに、プロトコル変換プログラム２００５は、例えば、SCSIとFCの様に、異なったストレージアクセスプロトコルを持つ装置が互いに交信できる様にもする。データセンタ１０１３外のネットワーク１０１２とデータセンタ１０１３内のネットワーク１０２５が、同じ種類の場合は、プロトコル変換プログラム２００５は省略可能である。

【００７８】実施例では、データは、データセンタ１０１３の外部からゲートウエイ１０１４を経由して受信され、ゲートウエイ１０１４を経由して外部ターゲットに送信される。ネットワーク１０１２とネットワーク１０２５が異なったプロトコルを使用している場合は、ゲー[illegible]

実施例では、スイッチ１０２６が受信アドレスで定義されたポートにパケットを送信する。

【００７９】送受信プログラム２００６は、ネットワークを経由した通信機能を提供する。ビューテーブル２００７は、ビュープログラム２００４が利用できる様に、多様なユーザに割り当てられたデータセンタ１０１３内のストレージに関する情報を維持しており、スイッチ１０２６内のメモリ１０２８に展開される。図８に示した実施例では、ユーザは、図６に示される様なデータセンタストレージの代表的なユーザイメージを持つことが出来る。

【００８０】図９は、本発明の一実施例での代表的なプログラムのブロックダイアグラムである。図９の実施例では、プログラムは、図１のストレージデバイス１０３８内のメモリ１０４０に展開される。図９の実施例で示されるように、通信プログラム９００１は、１つ以上のVPN (Virtual Private Network) プログラム２００２、認証プログラム２００３、ビュープログラム９００２、データIOプログラム９００３、及び送受信プログラム２００６を含む複数の要素プログラムプロセスで構成される。VPN プログラム２００２は、ユーザがパブリックネットワークを使用してデータセンタ１０１３内のボリュームにアクセスするのにプライベートネットワークを定義できる様にする。

【００８１】ユーザが、パブリックネットワークを使用してプライベートネットワークを定義するためのVPNを使用しない実施例では、VPN プログラム２００２は省略可能である。認証プログラム２００３は、データセンタ１０１３内のストレージデバイス１０３８内の情報にアクセスしようとしているユーザの認証を可能とする。ストレージデバイス１０３８がユーザ認証を行わない場合は、認証プログラム２００３は省略可能である。

【００８２】ビュープログラム９００２は、データセンタ１０１３内のデータ蓄積用ボリュームの仮想及び実アドレスの変換を実行する。データIOプログラム９００３は、ストレージデバイス１０３８に対する情報の読み書き動作を提供する。送受信プログラム２００６は、ネットワークを経由した通信機能を提供する。

【００８３】ビューテーブル２００７は、ビュープログラム２００４が利用できる様に、多様なユーザに割り当てられたデータセンタ１０１３内のストレージに関する情報を維持しており、ストレージデバイス１０３８内のメモリ１０４０に展開される。図９に示した実施例では、ユーザは、図６に示される様なデータセンタストレージの代表的なユーザイメージを持つことが出来る。

【００８４】図１０は、本発明の一実施例での代表的な通信プログラムのフローチャートである。図９で示した様に、実施例では、通信プログラム９００１は、ストレージデバイス１０３８内のメモリ１０４０に展開される。通信プログラム９００１は、データセンタ１０１３内のボリュームのひとつに蓄えられるべきデータを保有したデータパケットを受信し処理する。データパケットを受信後、ステップ１０００１にて、パケットは、例えば、グループAのクライアント１００２の様な、データセンタの外部から受信した内向きデータパケットか否かを判定する。

【００８５】データパケットがデータセンタ１０１３の外部から受信した場合は、処理はステップ１００１０に進み、そうでなければステップ１００１１に進む。データセンタ１０１３との接続にVPNを使用する場合は、オプションステップ１００１０にて、パケットはVPNプログラム２００２によって処理される。VPNを使用する実施例では、パブリックネットワークでデータを送信する前にデータを暗号化し、受信後に復号処理を行う。セキュリテイをより確実にする為、データのみならず送受信のネットワークアドレスについても暗号処理を適用する。

【００８６】したがって、VPNプログラム２００２はデータパケットのデータに加えて、追加的にアドレス情報についても復号処理を実施する。次に、オプションステップ１００００２にて、認証プログラム２００３により、パケットの認証確認がなされる。パケットが認証されると、処理はステップ１００００３に進む。そうでなければ、ステップ１００００７にてパケットは拒絶される。ステップ１００００３にて、ビュープログラム９００２が、ビューテーブル２００７の当該データパケット発信者のエントリにしたがって、データパケット内のアドレスとボリューム情報の変換を行う。内向きパケットの場合は、仮想ボリュームIDをボリュームIDに置き換える。

【００８７】本実施例での代表的なビュープログラムの処理例を図１１に示す。ステップ１００１２にて、ビュープログラム９００２の処理結果がチェックされる。ビュープログラム９００２が"no good (NG)"を返した場合は、パケットはステップ１００００７にて拒絶され、次のデータパケット処理の為にステップ１００００１に戻る。逆に、ビュープログラム９００２が"no good (NG)"を返さなかった場合は、ステップ１００００４にて、データIO処理が実施される。

【００８８】データIOプログラム９００３は、ストレージアクセスコマンドに従って、ボリュームからデータパケットへのRead処理か、データパケットからボリュームへのWrite処理かを実行する。データIO処理の完了後、次のデータパケット処理のためにステップ１００００１に戻る。

【００８９】ステップ１００００１にて、データパケットがデータセンタ１０１３の外部から受信されたものではなかった場合は、ステップ１００１１にて、当該データパケットはコマンドまたはデータを送信しているデータIOプログラム９００３から発信されたものか否かが判定

によって発信されたものなら、ステップ１０００５にて、ビュープログラム９００２が、ビューテーブル２００７の当該データパケット発信者のエントリにしたがって、データパケット内のアドレスとボリューム情報の変換を行う。外向きパケットの場合は、ボリュームIDを仮想ボリュームIDに置き換える。

【００９０】次に、ステップ１０００６にて、当該データパケットはデータセンタの外部に送信され、処理はステップ１０００１に戻って、次のデータパケット処理に備える。データパケットがデータIOプログラム９００３から送られたのではない場合は、ステップ１０００８にて、処理を終了して良いかを判定する。処理を終了する判定の場合は、処理を終了し、そうでない場合は、ステップ１０００９にて、エラー回復処理を実施した後に、ステップ１０００１に戻って次のデータパケット処理が実施される。ストレージデバイス１０３８がユーザ認証を行わない場合は、認証ステップ１０００２は省略可能である。

【００９１】図１１は、本発明の一実施例での代表的なビュープログラム処理のフローチャートである。実施例において、図１１のフローチャートで示したビュープログラム処理は、図９のビュープログラム９００２と図１０の処理ステップ１０００３及び１０００５に対応する。データパケット受信後、ステップ１１００１にて、本データパケットはデータセンタ１０１３より送信される外向きデータパケットか否かが判定される。

【００９２】本データパケットが外部からデータセンタ１０１３に向かうものなら、処理はステップ１１００２に進み、逆の場合は、ステップ１１００５に進む。次に、ステップ１１００２にて、本データパケットがストレージアクセスコマンドを有するか、有する場合は、本コマンドは仮想ボリュームID３００５を含むか否かが判定される。本データパケットが仮想ボリュームIDを含まなければ、処理はOK応答を伴って呼び出したプロセスに戻る。

【００９３】仮想ボリュームIDを含む場合は、ステップ１１００９にて、ビューテーブル２００７の内容をチェックして、当該仮想プライベートボリュームIDが当該パケットの送信ユーザに対して正しいか否かが判定される。不正仮想プライベートボリュームIDが検出されたら、処理は"no good"応答を呼び出したプロセスに返す。仮想ボリュームIDが正当な場合は、ステップ１１００３にて、ビューテーブル２００７を検索してパケット送信ユーザの仮想プライベートボリュームID３００５に対応するボリュームID３００６を求める。次に、ステップ１１００４にて、本データパケット内の仮想ボリュームID３００５をビューテーブル２００７から抽出したボリュームID３００６により置き換える。

【００９４】本データパケットがデータセンタ１０１３の外部から受信されたものではない場合は、本パケットは外向きパケットである。従って、判定ステップ１１００５にて、本データパケットはストレージアクセスコマンドとボリュームID３００６を有するかをチェックする。

【００９５】本データパケットがストレージアクセスコマンドを有し、本コマンドがボリュームID３００６を有する場合は、ステップ１１００６にて、ビューテーブル２００７を検索して当該ユーザのボリュームID３００６を検出する。ステップ１１００７にて、ボリュームID３００６は、ビューテーブル２００７よりユーザに対応して抽出した仮想ボリュームID３００５に置き換えられる。本データパケットがストレージアクセスコマンドとボリュームIDを含まない場合は、当該ユーザの受信アドレスを仮想受信アドレスに変換して、"OK"応答を呼び出したプロセスに返す。

【００９６】図１１に示した実施例では、ユーザは、図６に示される様なデータセンタストレージの代表的なユーザイメージを持つことが出来る。本発明のその他の実施例として、データセンタ内のゲートウエイ、サーバー、スイッチ、ストレージのような如何なる装置でも、同時にビユー変換機能を果たす事が出来る。

【００９７】これまで述べ来たことは、本発明の好適な実施例である。付記されている請求の範囲で定義された本発明の範囲を逸脱する事なく、変更と修正が可能である事は言うまでもない。

【００９８】

【発明の効果】本発明の実施により、ユーザは、仮想アドレスと仮想ボリューム識別子のシステムを用いて、ストレージデバイス内の資源にアクセスできる様になる。本発明の実施により、企業体を含めてユーザが、インターネットまたは他の種類のネットワークを経由して、ユーザのネットワークでSSP（Storage Service Provider）内のボリュームを使用することが可能になる。本発明の実施により、SSPとユーザは、ユーザのデータセンタのみならずSSP内のストレージデバイス、ボリューム、および機器の固有情報を隠蔽し、双方にとってプライバシを確立することができる。

【図面の簡単な説明】

【図１】本発明の一実施例でのSSP（Storage Service Provider）の代表的な構成を示すダイアグラムである。

【図２】本発明の一実施例での代表的なプログラムを示すブロックダイアグラムである。

【図３】本発明の一実施例でのビューテーブルの代表的なフォーマットを示す図である。

【図４】図４は、本発明の一実施例での代表的な通信プログラムを示すフローチャートである。

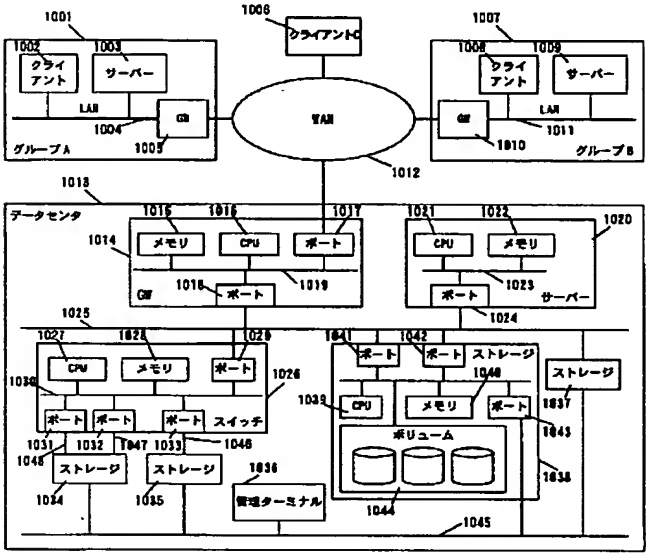
【図５】本発明の一実施例での代表的なビュープログラム処理を示すフローチャートである。

【図６】本発明の一実施例でのユーザに見える代表的なストレージシステムを示す図である。

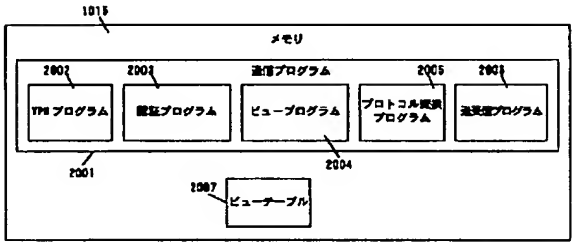
【図７】本発明の一実施例での代表的なプログラムを示すブロックダイアグラムである。
【図８】本発明の一実施例での代表的なプログラムを示すブロックダイアグラムである。
【図９】本発明の一実施例での代表的なプログラムを示すブロックダイアグラムである。
【図１０】本発明の一実施例での代表的な通信プログラムを示すフローチャートである。
【図１１】本発明の一実施例での代表的なビュープログラム処理を示すフローチャートである。
【符号の説明】

１００１、１００７･･･グループA、B、１００２、１００６、１００８･･･クライアント、１００３、１００９、１０２０･･･サーバー、１０１３･･･データセンタ、１０２６･･･　　スイッチ、１０３４，１０３５，１０３７，１０３８･･･ストレージ、１０４４･･･ボリューム、１０３６･･･管理ターミナル、２００１、９００１･･･通信プログラム、２００２･･･VPNプログラム、２００３･･･認証プログラム、２００４･･･ビュープログラム、２００５･･･プロトコル変換プログラム、２００６･･･送受信プログラム、９００３･･･データIOプログラム

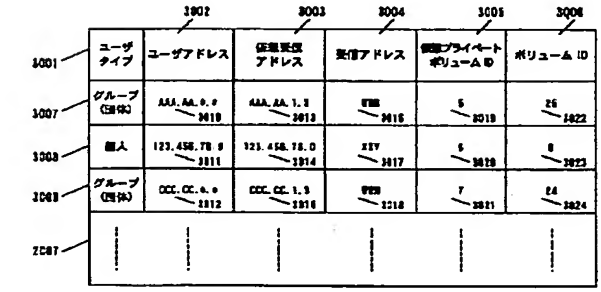
【図１】



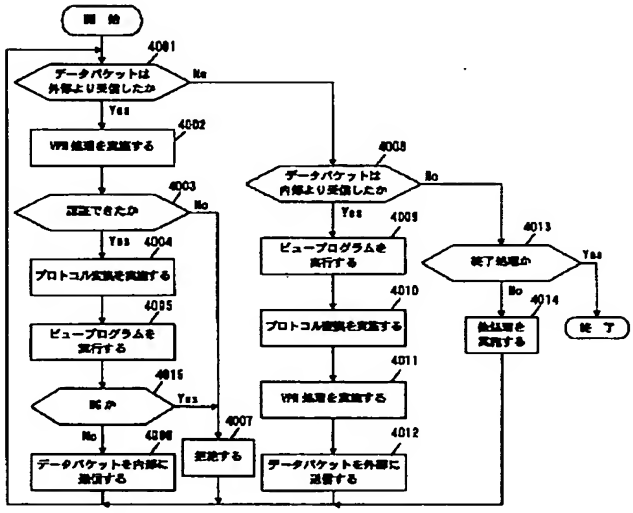
【図２】



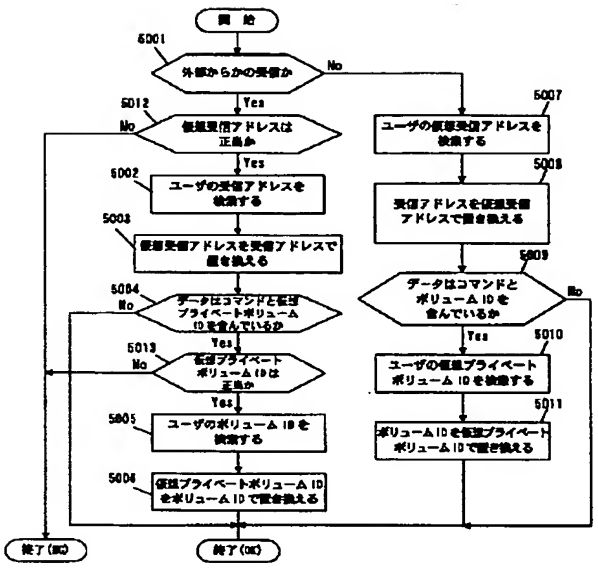
【図３】



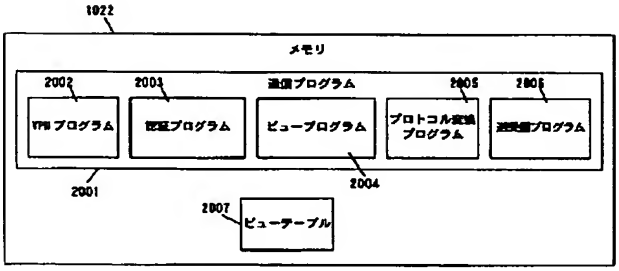
【図４】



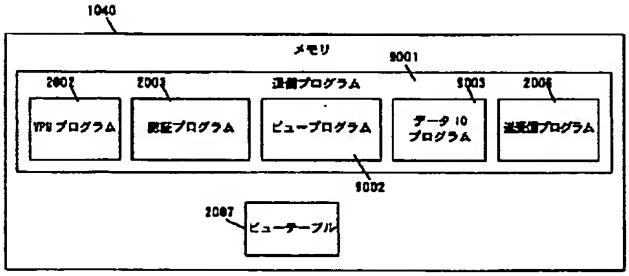
【図５】



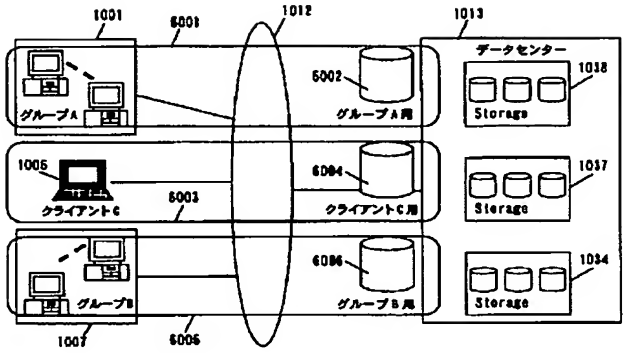
【図７】



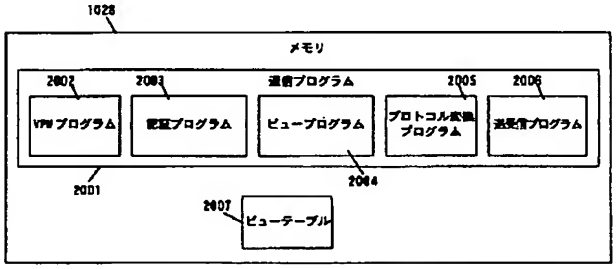
【図９】



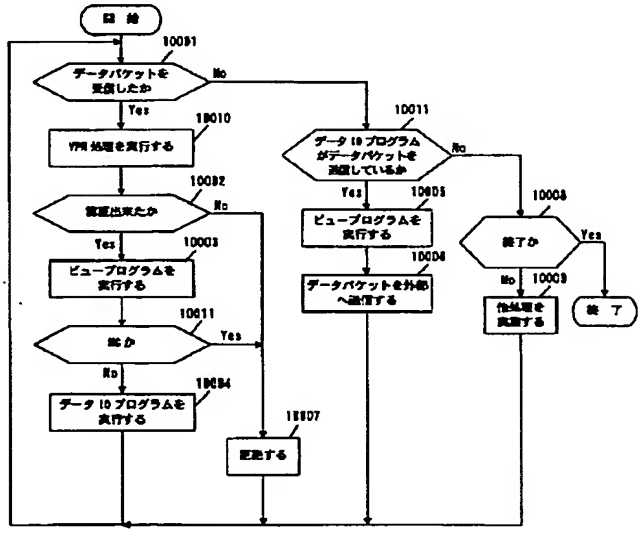
【図６】



【図８】

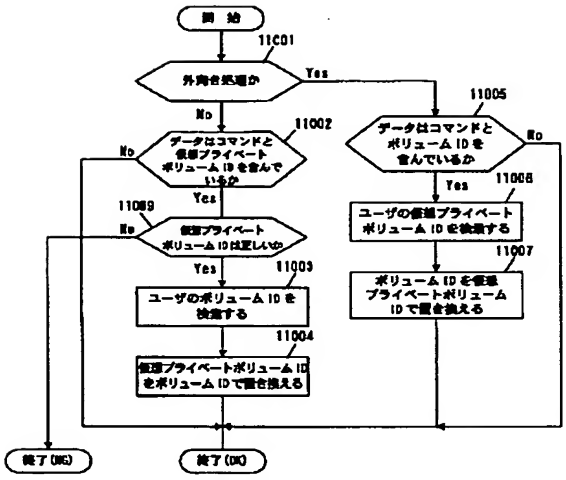


【図１０】



【図１１】

【図１１】


開始
11C01
外向き処理か
Yes
No
11002
データはコマンドと仮想プライベートボリューム ID を含んでいるか
No
Yes
11009
No
仮想プライベートボリューム ID は正しいか
Yes
11003
ユーザのボリューム ID を検索する
11004
仮想プライベートボリューム ID をボリューム ID で置き換える
11005
データはコマンドとボリューム ID を含んでいるか
No
Yes
11006
ユーザの仮想プライベートボリューム ID を検索する
11007
ボリューム ID を仮想プライベートボリューム ID で置き換える
終了(NG)
終了(OK)

【外国語明細書】

Virtual Private Volume Method and System

BACKGROUND OF THE INVENTION

The present invention relates generally to data storage systems, and in particular to techniques for controlling storage access based on a designated time.

The information technology revolution brings with it an ever increasing need for more storage capacity for business enterprises. It is expected that the average Fortune 1000 company's storage requirement will more than double in the coming years. In addition, growth has brought shortages of skilled persons in the information technology field. These challenges confront many companies facing the need to expand and improve their information technology assets. Increasingly, companies are turning to outsourcing storage management as a method of coping with the need to grow capacity in view of rapidly increasing demand. Storage Service Providers (SSPs) is one such service for providing storage infrastructure management to business enterprises. By subscribing to an SSP, companies can obtain needed storage resources by purchasing the services from the SSP. The SSP owns storage systems, which it uses to provide storage capacity for the users' host systems, as well as provide the storage management services. Users pay for the storage usage and management services based upon the terms of a service level agreement (SLA) made between the user and the SSP.

While certain advantages to present SSP technologies are perceived, opportunities for further improvement exist. For example, according to conventional SSP technology, the SSP provides storage resources for the host systems in the user's site in disk storage systems owned by the SSP at the site. However, some SSP users would like to locate their equipment remotely from the SSP site. For example, users may wish to access data held in the storage systems of the SSP via the Internet, or other network. Further, security is an important concern to both the user and the SSP. For the user, this means that valuable business information assets can be protected by restricting access to the data in storage. For the SSP, this means that data integrity is preserved for its

customers, and that no user receives access that is not authorized. For example, various divisions or departments in a large company may wish to have their own storage resources, which are private and therefore cannot be accessed by members of other divisions or departments.

What is needed are improved techniques for managing access to storage resources.

SUMMARY OF THE INVENTION

The present invention provides techniques for managing access to storage resources. In specific embodiments, storage devices provide storage resources to users using a system of virtual addresses and virtual volume identifiers. In select specific embodiments, a storage service provider (SSP) can make volumes available to a user, which may be a company, for example, in the user's network via the Internet or other kinds of network connections. In specific embodiments, the SSP and the user's data center can conceal the identity of the storage devices, volumes, and equipment of the SSP, as well as that of the user's data center in order to provide privacy to both user and storage provider.

In a representative specific embodiment according to the present invention, a storage apparatus is provided. The storage apparatus comprises a gateway, having a processor, a memory, and at least one port operative to connect to an external network; one or more devices that store information, each of the devices further comprising one or more volumes; a server; a switch; and an internal network connecting the gateway, the server, the switch, and the one or more devices that store information. The gateway receives a data packet for storing, and thereupon searches in the memory for a virtual destination address retrieved from the data packet, and thereupon reads from the memory a corresponding destination address for a particular one of the one or more devices that store information, and thereupon replaces in the data packet the virtual destination address with the corresponding destination address from the memory. In specific embodiments, the virtual destination address and the destination address are stored in a table. However, in other embodiments, these addresses, as well as volume identifiers and user identifiers may be stored in other types of data structures, such as link lists, queues, stacks, and so forth. Further, these data structures may be disposed in memory or stored in a disk storage, and the like.

In a specific embodiment, the gateway authenticates a source of the data packet based upon a user address in the data packet. In some specific embodiments, the external network comprises a virtual private network (VPN). In such embodiments, the gateway, for example, performs VPN processing for the data packet.

In specific embodiments, the external network uses a first protocol and the internal network uses a second protocol, which may be different from the first protocol. In such cases, the gateway, for example, translates the data packet from the first protocol to the second protocol. The first protocol can be any one of an IP protocol, ATM, and Fibre channel, protocols, for example, as well as any of a variety of other protocols known to those skilled in the art. Similarly, the second protocol comprises any one of the previously mentioned protocols.

In specific embodiments, the gateway searches in the data packet for a command and a virtual private volume identifier, and if found, thereupon searches in the memory for a volume identifier corresponding to the virtual private volume identifier, and thereupon replaces the virtual private volume identifier in the data packet with the volume identifier.

In specific embodiments, the gateway receives a data packet being sent to the external network, and thereupon searches in the memory for a destination address retrieved from the data packet, and thereupon reads from the memory a corresponding virtual destination address from the memory, and thereupon replaces in the data packet the destination address with the corresponding virtual destination address from the memory.

In an alternative specific embodiment according to the present invention, a storage apparatus is provided. The storage apparatus comprises a server, having a processor, a memory, and at least one port operative to connect to an external network; one or more devices that store information, each of the devices further comprising one or more volumes; a switch; and an internal network connecting the server, the switch, and the one or more devices that store information. The server receives a data packet for storing, and thereupon searches in the memory for a virtual destination address retrieved from the data packet, and thereupon reads from the memory a corresponding destination address for a particular one of the one or more devices that store information, and thereupon replaces in the data packet the virtual destination address with the corresponding destination address from the memory.

In an alternative specific embodiment according to the present invention, a storage apparatus is provided. The storage apparatus comprises a switch, having a processor, a memory, and at least one port operative to connect to an external network; one or more devices that store information, each of the devices further comprising one or more volumes; a server; and an internal network connecting the server, the switch, and the one or more devices that store information. The switch receives a data packet for storing, and thereupon searches in the memory for a virtual destination address retrieved from the data packet, and thereupon reads from the memory a corresponding destination address for a particular one of the one or more devices that store information, and thereupon replaces in the data packet the virtual destination address with the corresponding destination address from the memory.

In an alternative specific embodiment according to the present invention, a storage apparatus is provided. The storage apparatus comprises one or more devices that store information, each of the devices further comprising one or more volumes, a processor, a memory, and at least one port operative to connect to an external network; a switch; a server; and an internal network connecting the server, the switch, and the one or more devices that store information. The one or more devices that store information receives a data packet for storing, and thereupon searches in the memory for a virtual destination address retrieved from the data packet, and thereupon reads from the memory a corresponding destination address for a particular one of the one or more devices that store information, and thereupon replaces in the data packet the virtual destination address with the corresponding destination address from the memory.

In a representative specific embodiment according to the present invention, a method for managing storage is provided. The method comprises receiving a data packet; searching for a virtual destination address retrieved from the data packet; reading a corresponding destination address for a particular one of one or more devices that store information; and replacing in the data packet the virtual destination address with the corresponding destination address.

Numerous benefits are achieved by way of the present invention over conventional techniques. Specific embodiments according to the present invention can enable a storage service provider (SSP) to make volumes available to a user, which may be a company, for example, in the user's network via the Internet or other kinds of network connections. In specific embodiments, the SSP and the user's data center can

conceal the identity of the storage devices, volumes, and equipment of the SSP, as well as that of the user's data center in order to provide privacy to both user and storage provider.

These and other benefits are described throughout the present specification. A further understanding of the nature and advantages of the invention herein may be realized by reference to the remaining portions of the specification and the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig.1 illustrates a diagram of a representative configuration of an example storage service provider (SSP) in a specific embodiment of the present invention.

Fig. 2 illustrates a block diagram of representative programs in a specific embodiment of the present invention

Fig. 3 illustrates a diagram of a representative format of a view table in a specific embodiment of the present invention.

Fig. 4 illustrates a flow chart of a representative communication program in a specific embodiment of the present invention.

Fig. 5 illustrates a flow chart of a representative view program processing in a specific embodiment of the present invention.

Fig. 6 illustrates a diagram of a representative storage system as seen by a user in a specific embodiment of the present invention.

Fig. 7 illustrates a block diagram of representative programs in a specific embodiment of the present invention.

Fig. 8 illustrates a block diagram of representative programs in a specific embodiment of the present invention.

Fig. 9 illustrates a block diagram of representative programs in a specific embodiment of the present invention.

Fig. 10 illustrates a flow chart of a representative communication program in a specific embodiment of the present invention.

DESCRIPTION OF THE SPECIFIC EMBODIMENTS

The present invention provides techniques for managing access to storage resources. In specific embodiments, storage devices provide storage resources to users using a system of virtual addresses and virtual volume identifiers. In select specific

embodiments, a storage service provider (SSP) can make volumes available to a user, which may be a company, for example, in the user's network via the Internet or other kinds of network connections. In specific embodiments, the SSP and the user's data center can conceal the identity of the storage devices, volumes, and equipment of the SSP, as well as that of the user's data center in order to provide privacy to both user and storage provider.

Virtual Private Network (VPN) is a network technology for obtaining private network like environments using a public network, such as the Internet. Two or more networks can connect via the Internet and communicate with each other as one private network using VPN. One noteworthy limitation to conventional VPN technologies is that they do not conceal the identity of all equipment in the networks that comprise the virtual private network.

Zoning technology is a Fibre Channel (FC) switching technology. Zoning technology enables a port to be assigned to an other port, enabling equipment connected to one port to be able to use volumes that are connected to other ports to be assigned to that port. Conventionally, each piece of equipment connects to the FC switch directly. Further, conventional zoning techniques do not conceal the identity of volumes which are connected to a common port and may be used by other equipment.

Logical Unit Number (LUN) security is a storage technology in which a storage device connected by a Fibre Channel, for example, detects equipment identities, called World Wide Names (WWN), so that the identity of volumes within the storage devices are protected from unauthorized access. Conventionally, each piece of equipment connects to the FC switch directly. Further, in conventional approaches, users may be aware of a LUN and port address.

Fig.1 illustrates a diagram of a representative configuration of an example storage service provider (SSP) in a specific embodiment of the present invention. Group A 1001 indicates a user's local network. Group B 1007 indicates another user's local network. Client C 1006 indicates a personal user. A data center 1013 comprises equipment of a storage provider, which can be an SSP, in a specific embodiment. The data center 1013 has at least one gateway1014 and at least one storage 1038. Users can connect to data center 1013 via a wide area network (WAN) 1012. WAN 1012 can be for example, the Internet, an ATM leased line, and so on. Each user can use the same network for connecting to the data center 1013, for example. The users can use their own

leased line for connecting to the data center 1013 directory, as well. Gateway 1014 has at least one port 1017 for connecting to network 1012 outside of the data center 1013. Gateway 1014 has at least one port 1018 for connecting to network 1025 inside of the data center 1013. Network 1025 is used for accessing storage devices. Storage 1038 has at least one port 1042 for connecting to network 1025. Volumes 1044 are defined for the storage 1038, and have volume IDs that can be for example a Logical Unit Number (LUN) defined by the Small Computer System Interface (SCSI) protocol, for example. Port 1043 is connected to network 1045, and is used for management. Management terminal 1036 is connected to storage 1038, 1037, 1034, 1035 via network 1045, and is used to define the storage configuration. Switch 1026 has at least one port 1029 for connecting to the network 1025. Switch 1026 also has at least one port 1031 for connecting to the storage 1034. In another specific embodiment, in which the network 1025 and network 1045 are of the same type, for example both are IP networks, network 1025 and network 1045 can be integrated into one network. In another specific embodiment, in which the network 1012 is of a different type than network 1025, for example network 1012 is an IP network and network 1025 is a Fibre Channel (FC) network, the gateway 1014 provides a protocol exchange function between these different types of networks. In a specific embodiment in which the storage 1034 supports networks of different types, for example network 1025 is an IP network and a network 1048 is an FC network, switch 1026 provides protocol exchange functions between the different protocols. In such specific embodiments, the storage 1034 and storage 1038 support different network protocols. For example, in a specific embodiment in which network 1048 and network 1046 support different protocols, and network 1046 uses the same protocol as network 1025, the switch 1026 can provide protocol exchange functions. Further, the storage 1034 and the storage 1038 can support different network protocols and may use different storage access protocols, as well. In another specific embodiment, in which network 1048 and network 1046 use different network protocols and the storage 1034 and the storage 1035 communicate via switch 1026, the switch 1026 can provide protocol exchange function. Further, the storage 1034 and storage 1038 can support different network protocols and may use different storage access protocols, as well. In specific embodiments, the data center 1013 can be configured such that switch 1026, server 1020, or both are not included.

Fig. 2 illustrates a block diagram of representative programs in a specific embodiment of the present invention. In a specific embodiment, the programs illustrated by Fig. 2 are disposed in the memory 1015 of gateway 1014 in Fig. 1. As shown by Fig. 2, in a specific embodiment, a communication program 2001 comprises a plurality of component program processes, including one or more of a virtual private network (VPN) program 2002, an authentication program 2003, a view program 2004, a protocol exchanger program 2005 and a send and receive program 2006. A virtual private network (VPN) program 2002 enables the user to define a private network for accessing volumes within the data center 1013 using a public network. In a specific embodiment in which a user does not use the virtual private network (VPN) for defining a private network using a public network, the VPN program 2002 may be omitted. An authentication program 2003 provides the capability to authenticate the identity of a user who attempts to access information in one of the storage devices 1034 of the data center 1013. In a specific embodiment in which the gateway 1014 does not check user identity, the authentication program 2003 may be omitted. A view program 2004 provides translation of virtual and real addresses of volumes for storing data in the data center 1013. A protocol exchanger program 2005 provides protocol exchange functions that enable apparatus connected by networks of different topologies communicate with each other, such as for example an IP network communicating with an FC network. Further, the protocol exchanger program 2005 enables apparatus which use different storage access protocols, such as for example, SCSI and FC, to communicate with each other. In a specific embodiment, in which network 1012, external to data center 1013, and network 1025, internal to data center 1013, are of the same kind, the protocol exchanger program 2005 may be omitted. A send and receive program 2006 provides communications functions along the network. A view table 2007, which maintains information about storage in the data center 1013 that is allocated to various users for view program 2004, is also disposed in memory 1015.

Fig. 3 illustrates a diagram of a representative format of a view table in a specific embodiment of the present invention. As shown by Fig. 3, in a specific embodiment, the view table 2007 comprises a plurality of information fields for users. A user type 3001 indicates information about the user. A user address 3002 indicates an address of an individual user's machine, or a group of addresses for multiple users. For example, when the user type 3001 is set to "group," such as for user group 3007, users belonging to the group 3007 are defined by a common set of user addresses 3010, which

have access to the same volume in the data center 1013. When the user type 3001 is set to "personal," such as for personal user 3008, then that user is defined by a user address 3011, which can access a volume in the data center 1013. A Virtual Destination Address (VDA) 3003 is used by the user to specify a storage unit known to the user. The storage device has a volume, also known to the user, in which the user's information is stored. In a specific embodiment in which a user uses VPN to access data center 1013, the virtual destination address (VDA) is an IP address in a private network defined by the user using VPN. A destination address 3004 is an address of a storage device in the data center 1013, which is not known to the user. For example, the destination address 3004 can be an IP address, a hostname, a World Wide Name (WNN) for a fibre channel network, and so forth. When a storage unit has more than two ports for connecting to a network, then the storage unit will have a destination address 3004 for each port. A virtual private volume ID 3005 is used by user's to specify a volume that the user wishes to access. A volume ID 3006 is a volume ID that is not known to the user. Volume ID 3006 may be, for example a Logical Unit Number (LUN) defined by the SCSI protocol in various specific embodiments. The storage unit accesses the volume using the volume ID 3006.

Fig. 4 illustrates a flow chart of a representative communication program in a specific embodiment of the present invention. As shown in Fig. 4, in a specific embodiment, communication program 2001 resides in memory 1015 of gateway 1014. The communication program 2001 receives and processes data packets containing data to be stored on one of the volumes of the data center 1013. After a data packet is received, a check is made whether the data packet is an inbound data packet that was received from a source external to data center 4001, such as from client 1002 of Group A, for example. If the packet was received from outside of the data center 1013, then processing continues with step 4002. Otherwise, processing continues with step 4008. In an optional step 4002, the packet is processed by the virtual private network program 2002, in specific embodiments that use virtual private network to connect with data center 1013. In specific embodiments, using a virtual private network involves encrypting data before sending it through the public network and decrypting it at the receiving end. An additional level of security involves encrypting not only the data but also the originating and receiving network addresses. Accordingly, in specific embodiments, the virtual private network program 2002 performs decryption of data, and optionally address information, in the data packet. Next, the packet may be authenticated by an

authentication program 2003 in an optional step 4003. If the packet passes authentication, then processing continues with a step 4004. Otherwise, the packet is rejected in a step 4007. In optional step 4004, the protocol exchanger program 2005 performs any protocol translation required. For example, transforming data packet format, address formats, and so forth. Then, in a step 4005, view program 2005 translates address and volume information in the data packet according to an entry for the user originating the data packet in the view table 2007. For inbound packets, the virtual destination address is replaced by a destination address and virtual volume ID is replaced with a volume ID. A representative view program process is illustrated by Fig. 5 for a specific embodiment. In a step 4015, a result of view program 2005 processing is checked. If the view program returned "no good (NG)," then the packet is rejected in step 4007, and processing continues with step 4001 for the next data packet. Otherwise, if the view program did not return "no good," then in a step 4006, the packet is sent to network 1025 inside the data center, and processing continues with step 4001 for the next data packet.

If the data packet was not received from outside of the data center 1013, then in a step 4008, a check is made to determine if the data packet is outbound information received from inside the data center 1013. If the packet was received from inside the data center 1013, such as from storage 1038, for example, then in a step 4009, the view program 2005 view program 2005 translates address and volume information in the data packet according to an entry for the user originating the data packet in the view table 2007. For outbound packets, destination address is replaced by a virtual destination address and volume ID is replaced with a virtual volume ID. Otherwise, in a step 4013, a decision is made whether to terminate processing, or perform an error recovery task in step 4014 prior to continuing with step 4001 for the next data packet. Then, in an optional step 4010, in a specific embodiment, the protocol of the data packet is exchanged, if needed. Then, in an optional step 4011, in a specific embodiment that uses VPN, the VPN program 2002 processes the data packet. The virtual private network program 2002 performs encryption of data, and optionally address information, in the data packet. Then, in a step 4012, the data packet is sent to network 1012 outside of data center 1013. In a specific embodiment in which VPN is not supported or is not used, the VPN processing steps 4002 and 4011 may be omitted. In a specific embodiment in which the network 1012 outside of the data center 1013 and the network 1025 inside of the data

center 1013 are of the same type, the protocol exchange steps 4004 and 4010 may be omitted. In a specific embodiment in which the gateway does not check user identity, the authentication step 4003 may be omitted.

Fig. 5 illustrates a flow chart of a representative view program processing in a specific embodiment of the present invention. In specific embodiments, view program processing illustrated by the flow chart of Fig. 5 corresponds to view program 2004 of Fig. 2, and processing of steps 4005 and 4009 of Fig. 4. In a specific embodiment, after a data packet is received, a check is made whether the data packet is an inbound data packet that was received from a source outside of data center 1013 in a step 5001. If the data packet is from a source external to the data center 1013, then in a step 5012, a determination is made whether a virtual destination address 3003, which is a user defined storage address that is known to and used by the user, is the correct address for the user. This may be performed by referring to the view program table 2007, which provides the known correct addresses for each user. In a specific embodiment, the virtual destination address 3003 is checked to see if it is the correct address for the user that sent the data packet. If the virtual destination address 3003 is not correct, then processing returns a "no good" (NG) return condition to the invoking process. Otherwise, in a step 5002, the view table 2007 of Fig. 3 is searched for a destination address 3004 corresponding to the virtual destination address 3003 embedded in the data packet. Then, in a step 5003, the virtual destination address 3003 in the data packet is replaced by the destination address 3004 from view table 2007. Then, in a step 5004, a determination is made whether the data packet includes a storage access command, and if so, whether that command includes a virtual volume ID 3005. If the data packet does not include a virtual volume ID, then processing returns to an invoking process with an OK state, having translated the virtual destination address 3003 into a destination address 3004 in the data packet. Otherwise, in a step 5013, a determination is made whether the virtual private volume ID for the user who sent the data packet is correct, again by checking the contents of the view table 2007. If an incorrect virtual private volume ID is discovered, then processing returns a "no good" return condition to an invoking process. Otherwise, in a step 5005, the view table 2007 is searched for the volume ID 3006 corresponding to the virtual private volume ID 3005 for the user who sent the packet. Then, in a step 5006, the virtual volume ID 3005 in the data packet is replaced with a volume ID 3006 retrieved from the view table 2007.

If the data packet was not received from outside of the data center 1013, then it is an outbound packet. Accordingly, in a step 5007, the view table 2007 is searched for the virtual destination address 3003 for the user to whom the data packet is being sent. Then, in a step 5008, the destination address 3004 in the data packet is replaced with a virtual destination address 3003 for the user retrieved from the view table 2007. Then, in a decisional step 5009, a determination is made whether the data packet includes a storage access command and a volume ID 3006. If the data packet includes a storage access command, and that command includes a volume ID 3006, then the view table 2007 is searched for the volume ID 3006 for the user in a step 5010. The volume ID 3006 is replaced with the corresponding virtual volume ID 3005 for the user retrieved from the view table 2007 in a step 5011. Otherwise, if the data packet does not include a storage access command and volume ID, then the processing returns an "OK" condition to an invoking process, having translated the destination address for the user into a virtual destination address and the volume ID into a virtual volume ID in the data packet. In a specific embodiment in which gateway 1014 does not handle volume ID, steps 5004, 5005, 5006, 5009, 5010, 5011, and 5013 may be omitted.

Fig. 6 illustrates a diagram of a representative storage system as seen by a user in a specific embodiment of the present invention. As shown by Fig. 6, the data center 1013 comprises a plurality of volumes for storing information. In a specific embodiment, these volumes can be allocated among a plurality of storage units, such as storage units 1034, 1037 and 1038, for example. A plurality of users access information on various volumes within data center 1013, by connecting to the data center 1013 by one or more networks 1012. For example, a user, group A 1001, connects via virtual destination address 6001 via the wide area network 1012 to data center 1013. Group A 1001 is presented with an image of their storage as a virtual volume 6002. Another user, group B 1007, connects via a virtual destination address 6005 via wide area network 1012 to the data center 1013. Similarly, group B 1007 is presented with an image of their storage as a virtual volume 6006. Individual user, client C 1006, connects via virtual destination address 6003 via the wide area network 1012 to data center 1013. User C 1006 is presented with an image of their storage as a virtual volume 6004. Accordingly, the data center 1013 appears like an individual volume to each user. Further, each user is blocked from seeing storage volumes of another user inside of data center 1013.

Fig. 7 illustrates a block diagram of representative programs in a specific embodiment of the present invention. In an alternative embodiment, the programs illustrated by Fig. 7 are disposed in the memory 1022 of server 1024 in Fig. 1. As shown by Fig. 7, in a specific embodiment, a communication program 2001 comprises a plurality of component program processes, including one or more of a virtual private network (VPN) program 2002, an authentication program 2003, a view program 2004, a protocol exchanger program 2005 and a send and receive program 2006. A virtual private network (VPN) program 2002 enables the user to define a private network for accessing volumes within the data center 1013 using a public network. In a specific embodiment in which a user does not use the virtual private network (VPN) for defining a private network using a public network, the VPN program 2002 may be omitted. An authentication program 2003 provides the capability to authenticate the identity of a user who attempts to access information in one of the storage devices 1034 of the data center 1013. In a specific embodiment in which the server 1024 does not check user identity, the authentication program 2003 may be omitted. A view program 2004 provides translation of virtual and real addresses of volumes for storing data in the data center 1013. A protocol exchanger program 2005 provides protocol exchange functions that enable apparatus which use different storage access protocols, such as for example, SCSI and FC, to communicate with each other. In a specific embodiment in which the user's apparatus and the storage apparatus of the data center 1013 use same kind of storage access protocol, the protocol exchanger program 2005 may be omitted. In a specific embodiment in which network 1012 and network 1025 use different network protocols, for example, network 1012 uses an IP network protocol and network 1025 uses Fibre channel, the gateway 1014 performs protocol exchange functions between these different types of network protocols. In a specific embodiment, data is received from sources external to the data center 1013 via the gateway 1014, and sent to these external targets via the gateway 1014. A send and receive program 2006 provides communications functions along the network. A view table 2007, which maintains information about storage in the data center 1013 that is allocated to various users for view program 2004, is also disposed in memory 1022 of server 1024. A specific embodiment, as illustrated by Fig. 7, enables users to have the representative user image of the data center storage as illustrated by Fig. 6.

Fig. 8 illustrates a block diagram of representative programs in a specific embodiment of the present invention. In an alternative embodiment, the programs .

illustrated by Fig. 8 are disposed in the memory 1028 of switch 1026 in Fig. 1. As shown by Fig. 8, in a specific embodiment, a communication program 2001 comprises a plurality of component program processes, including one or more of a virtual private network (VPN) program 2002, an authentication program 2003, a view program 2004, a protocol exchanger program 2005 and a send and receive program 2006. A virtual private network (VPN) program 2002 enables the user to define a private network for accessing volumes within the data center 1013 using a public network. In a specific embodiment in which a user does not use the virtual private network (VPN) for defining a private network using a public network, the VPN program 2002 may be omitted. An authentication program 2003 provides the capability to authenticate the identity of a user who attempts to access information in one of the storage devices 1034 of the data center 1013. In a specific embodiment in which the switch 1026 does not check user identity, the authentication program 2003 may be omitted. A view program 2004 provides translation of virtual and real addresses of volumes for storing data in the data center 1013. A protocol exchanger program 2005 provides protocol exchange functions that enable apparatus connected by networks of different topologies communicate with each other, such as for example an IP network communicating with an FC network. Further, the protocol exchanger program 2005 enables apparatus which use different storage access protocols, such as for example, SCSI and FC, to communicate with each other. In a specific embodiment, in which network 1012, external to data center 1013, and network 1025, internal to data center 1013, are of the same kind, the protocol exchanger program 2005 may be omitted. In a specific embodiment, data is received from sources external to the data center 1013 via the gateway 1014, and sent to these external targets via the gateway 1014. In a specific embodiment in which network 1012 and network 1025 use different network protocols, gateway 1014 performs protocol exchange function. In this specific embodiment, switch 1026 sends packets to a port which is defined by the destination address. A send and receive program 2006 provides communications functions along the network. A view table 2007, which maintains information about storage in the data center 1013 that is allocated to various users for view program 2004, is also disposed in memory 1028 of switch 1026. A specific embodiment, as illustrated by Fig. 8, enables users to have the representative user image of the data center storage as illustrated by Fig. 6.

Fig. 9 illustrates a block diagram of representative programs in a specific embodiment of the present invention. In an alternative embodiment, the programs

illustrated by Fig. 9 are disposed in the memory 1040 of storage device 1038 in Fig. 1. As shown by Fig. 9, in a specific embodiment, a communication program 9001 comprises a plurality of component program processes, including one or more of a virtual private network (VPN) program 2002, an authentication program 2003, a view program 9002, a data IO program 9003 and a send and receive program 2006. A virtual private network (VPN) program 2002 enables the user to define a private network for accessing volumes within the data center 1013 using a public network. In a specific embodiment in which a user does not use the virtual private network (VPN) for defining a private network using a public network, the VPN program 2002 may be omitted. An authentication program 2003 provides the capability to authenticate the identity of a user who attempts to access information in one of the storage devices 1038 of the data center 1013. In a specific embodiment in which the storage device 1038 does not check user identity, the authentication program 2003 may be omitted. A view program 9002 provides translation of virtual and real addresses of volumes for storing data in the data center 1013. A data IO program 9003 provides reading and writing of information to and from storage device 1038. A send and receive program 2006 provides communications functions along the network. A view table 2007, which maintains information about storage in the data center 1013 that is allocated to various users for view program 2004, is also disposed in memory 1040 of storage 1038. A specific embodiment, as illustrated by Fig. 9, enables users to have the representative user image of the data center storage as illustrated by Fig. 6.

Fig. 10 illustrates a flow chart of a representative communication program in a specific embodiment of the present invention. As shown in Fig. 10, in a specific embodiment, communication program 9001 resides in memory 1040 of storage device 1038. The communication program 9001 receives and processes data packets containing data to be stored on one of the volumes of the data center 1013. After a data packet is received, a check is made whether the data packet is an inbound data packet that was received from a source external to data center 10001, such as from client 1002 of Group A, for example. If the packet was received from outside of the data center 1013, then processing continues with step 10002. Otherwise, processing continues with step 10008. In an optional step 10010, the packet is processed by the virtual private network program 2002, in specific embodiments that use virtual private network to connect with data center 1013. In specific embodiments, using a virtual private network involves encrypting data

before sending it through the public network and decrypting it at the receiving end. An additional level of security involves encrypting not only the data but also the originating and receiving network addresses. Accordingly, in specific embodiments, the virtual private network program 2002 performs decryption of data, and optionally address information, in the data packet. Next, the packet may be authenticated by an authentication program 2003 in an optional step 10002. If the packet passes authentication, then processing continues with a step 10003. Otherwise, the packet is rejected in a step 10007. In a step 1003, view program 9002 translates address and volume information in the data packet according to an entry for the user originating the data packet in the view table 2007. For inbound packets, the virtual volume ID is replaced with a volume ID. A representative view program process is illustrated by Fig. 11 for a specific embodiment. In a step 10011, a result of view program 9002 processing is checked. If the view program 9002 returned "no good (NG)," then the packet is rejected in step 10007, and processing continues with step 10001 for the next data packet. Otherwise, if the view program 9002 did not return "no good," then in a step 10004, data IO processing is performed. Data IO program 9003 reads information from a data packet to a volume or writes information from a data packet to a volume according to a storage access command. After data IO processing, processing continues with step 10001 for the next data packet.

If in step 10001, it is determined that the data packet was not received from outside of the data center 1013, then in a decisional step 10011, a determination is made whether the data packet is from the data IO program 9003 sending a command or data. If the data packet was sent by the data IO program 9003, then, in a step 10005, a view program 9002 translates address and volume information in the data packet according to an entry for the user originating the data packet in the view table 2007. For outbound packets, the volume ID is replaced with a virtual volume ID. Then, in a step 10006, the data packet is sent outside of the data center, and processing continues with step 10001 for the next data packet. Otherwise, if the data packet was not sent by the data IO program 9003, then in a step 10008, a check is made to determine whether to terminate processing. If the decision is made to terminate processing, then the processing is terminated. Otherwise, an error recovery process is performed in a step 10009, and then processing continues with another data packet in step 10001. In a specific

embodiment in which the storage 1038 does not check user identity, authentication step 10002 may be omitted.

Fig. 11 illustrates a flow chart of a representative view program processing in a specific embodiment of the present invention. In specific embodiments, view program processing illustrated by the flow chart of Fig. 11 corresponds to view program 9002 of Fig. 9, and processing of steps 10003 and 10005 of Fig. 10. In a specific embodiment, after a data packet is received, a check is made whether the data packet is an outbound data packet that being sent from the data center 1013 in a step 11001. If the data packet is from a source external to the data center 1013, then Otherwise, processing continues with a step 11005. Then, in a step 11002, a determination is made whether the data packet includes a storage access command, and if so, whether that command includes a virtual volume ID 3005. If the data packet does not include a virtual volume ID, then processing returns to an invoking process with an OK state. Otherwise, in a step 11009, a determination is made whether the virtual private volume ID for the user who sent the packet is correct, again by checking the contents of the view table 2007. If an incorrect virtual private volume ID is discovered, then processing returns a "no good" return condition to an invoking process. Otherwise, in a step 11003, the view table 2007 is searched for the volume ID 3006 corresponding to the virtual private volume ID 3005 for the user who sent the packet. Then, in a step 11004, the virtual volume ID 3005 in the data packet is replaced with a volume ID 3006 retrieved from the view table 2007.

If the data packet was not received from outside of the data center 1013, then it is an outbound packet. Accordingly, in a decisional step 11005, a determination is made whether the data packet includes a storage access command and a volume ID 3006. If the data packet includes a storage access command, and that command includes a volume ID 3006, then the view table 2007 is searched for the volume ID 3006 for the user in a step 11006. The volume ID 3006 is replaced with the corresponding virtual volume ID 3005 for the user retrieved from the view table 2007 in a step 11007. Otherwise, if the data packet does not include a storage access command and volume ID, then the processing returns an "OK" condition to an invoking process, having translated the destination address for the user into a virtual destination address and the volume ID into a virtual volume ID in the data packet. A specific embodiment, as illustrated by Fig. 11, enables users to have the representative user image of the data center storage as illustrated by Fig. 6.

In according to other embodiment of the invention, these equipment in data center, like a gateway, server, switch, and storage, any equipment has these view change function at same time.

The preceding has been a description of the preferred embodiment of the invention. It will be appreciated that deviations and modifications can be made without departing from the scope of the invention, which is defined by the appended claims.

What is claimed is:

1. A storage apparatus comprising:

a gateway, having a processor, a memory, and at least one port operative to connect to an external network;

at least one of a plurality of devices that store information, each of said devices further comprising at least one of a plurality of volumes;

a server;

a switch; and

an internal network connecting said gateway, said server, said switch, and said at least one of a plurality of devices that store information; wherein

said gateway receives a data packet for storing, and thereupon searches in said memory for a virtual destination address retrieved from said data packet, and thereupon reads from said memory a corresponding destination address for a particular one of said at least one of a plurality of devices that store information, and thereupon replaces in said data packet said virtual destination address with said corresponding destination address from said memory.

2. The apparatus of claim 1, wherein said gateway authenticates a source of said data packet based upon a user address in said data packet.

3. The apparatus of claim 1, wherein said external network comprises a virtual private network (VPN), and wherein said gateway performs VPN processing for said data packet.

4. The apparatus of claim 1, wherein said external network uses a first protocol and said internal network uses a second protocol, and wherein said gateway translates said data packet from said first protocol to said second protocol.

5. The apparatus of claim 4, wherein said first protocol comprises at least one of IP protocol, ATM, and Fibre channel.

6. The apparatus of claim 4, wherein said second protocol comprises at least one of IP protocol, ATM, and Fibre channel.

7. The apparatus of claim 1, wherein said gateway searches in said data packet for a command and a virtual private volume identifier, and if found, thereupon searches in said memory for a volume identifier corresponding to said virtual private volume identifier, and thereupon replaces said virtual private volume identifier in said data packet with said volume identifier.

8. The apparatus of claim 1, wherein said gateway receives a data packet being sent to said external network, and thereupon searches in said memory for a destination address retrieved from said data packet, and thereupon reads from said memory a corresponding virtual destination address from said memory, and thereupon replaces in said data packet said destination address with said corresponding virtual destination address from said memory.

9. The apparatus of claim 1, wherein said virtual destination address and said destination address are stored in a table.

10. A storage apparatus comprising:

a server, having a processor, a memory, and at least one port operative to connect to an external network;

at least one of a plurality of devices that store information, each of said devices further comprising at least one of a plurality of volumes;

a switch; and

an internal network connecting said server, said switch, and said at least one of a plurality of devices that store information; wherein

said server receives a data packet for storing, and thereupon searches in said memory for a virtual destination address retrieved from said data packet, and thereupon reads from said memory a corresponding destination address for a particular one of said at least one of a plurality of devices that store information, and thereupon replaces in said data packet said virtual destination address with said corresponding destination address from said memory.

11. The apparatus of claim 10, further comprising a gateway, said gateway having a processor, a memory, and at least one port operative to connect to an external network, and wherein said external network uses a first protocol and said internal

network uses a second protocol, and wherein said gateway translates said data packet from said first protocol to said second protocol.

12. The apparatus of claim 11, wherein said first protocol comprises at least one of IP protocol, ATM, and Fibre channel.

13. The apparatus of claim 11, wherein said second protocol comprises at least one of IP protocol, ATM, and Fibre channel.

14. The apparatus of claim 11, wherein said external network comprises a virtual private network (VPN), and wherein said gateway performs VPN processing for said data packet.

15. The apparatus of claim 10, wherein said server searches in said data packet for a command and a virtual private volume identifier, and if found, thereupon searches in said memory for a volume identifier corresponding to said virtual private volume identifier, and thereupon replaces said virtual private volume identifier in said data packet with said volume identifier.

16. The apparatus of claim 10, wherein said server receives a data packet being sent to said external network, and thereupon searches in said memory for a destination address retrieved from said data packet, and thereupon reads from said memory a corresponding virtual destination address from said memory, and thereupon replaces in said data packet said destination address with said corresponding virtual destination address from said memory.

17. The apparatus of claim 10, wherein said server authenticates a source of said data packet based upon a user address in said data packet.

18. A storage apparatus comprising:

a switch, having a processor, a memory, and at least one port operative to connect to an external network;

at least one of a plurality of devices that store information, each of said devices further comprising at least one of a plurality of volumes;

a server; and

an internal network connecting said server, said switch, and said at least one of a plurality of devices that store information; wherein

said switch receives a data packet for storing, and thereupon searches in said memory for a virtual destination address retrieved from said data packet, and thereupon reads from said memory a corresponding destination address for a particular one of said at least one of a plurality of devices that store information, and thereupon replaces in said data packet said virtual destination address with said corresponding destination address from said memory.

19. The apparatus of claim 18, further comprising a gateway, said gateway having a processor, a memory, and at least one port operative to connect to an external network, and wherein said external network uses a first protocol and said internal network uses a second protocol, and wherein said gateway translates said data packet from said first protocol to said second protocol.

20. The apparatus of claim 19, wherein said first protocol comprises at least one of IP protocol, ATM, and Fibre channel.

21. The apparatus of claim 19, wherein said second protocol comprises at least one of IP protocol, ATM, and Fibre channel.

22. The apparatus of claim 19, wherein said external network comprises a virtual private network (VPN), and wherein said gateway performs VPN processing for said data packet.

23. The apparatus of claim 18, wherein said switch searches in said data packet for a command and a virtual private volume identifier, and if found, thereupon searches in said memory for a volume identifier corresponding to said virtual private volume identifier, and thereupon replaces said virtual private volume identifier in said data packet with said volume identifier.

24. The apparatus of claim 18, wherein said switch receives a data packet being sent to said external network, and thereupon searches in said memory for a destination address retrieved from said data packet, and thereupon reads from said memory a corresponding virtual destination address from said memory, and thereupon

replaces in said data packet said destination address with said corresponding virtual destination address from said memory.

25. The apparatus of claim 18, wherein said switch authenticates a source of said data packet based upon a user address in said data packet.

26. A storage apparatus comprising:

at least one of a plurality of devices that store information, each of said devices further comprising at least one of a plurality of volumes, a processor, a memory, and at least one port operative to connect to an external network;

a switch;

a server; and

an internal network connecting said server, said switch, and said at least one of a plurality of devices that store information; wherein

said at least one of a plurality of devices that store information receives a data packet for storing, and thereupon searches in said memory for a virtual destination address retrieved from said data packet, and thereupon reads from said memory a corresponding destination address for a particular one of said at least one of a plurality of devices that store information, and thereupon replaces in said data packet said virtual destination address with said corresponding destination address from said memory.

27. The apparatus of claim 26, further comprising a gateway, said gateway having a processor, a memory, and at least one port operative to connect to an external network, and wherein said external network uses a first protocol and said internal network uses a second protocol, and wherein said gateway translates said data packet from said first protocol to said second protocol.

28. The apparatus of claim 27, wherein said first protocol comprises at least one of IP protocol, ATM, and Fibre channel.

29. The apparatus of claim 27, wherein said second protocol comprises at least one of IP protocol, ATM, and Fibre channel.

30. The apparatus of claim 27, wherein said external network comprises a virtual private network (VPN), and wherein said gateway performs VPN processing for said data packet.

31. The apparatus of claim 26, wherein said at least one of a plurality of devices that store information searches in said data packet for a command and a virtual private volume identifier, and if found, thereupon searches in said memory for a volume identifier corresponding to said virtual private volume identifier, and thereupon replaces said virtual private volume identifier in said data packet with said volume identifier.

32. The apparatus of claim 26, wherein said at least one of a plurality of devices that store information receives a data packet being sent to said external network, and thereupon searches in said memory for a destination address retrieved from said data packet, and thereupon reads from said memory a corresponding virtual destination address from said memory, and thereupon replaces in said data packet said destination address with said corresponding virtual destination address from said memory.

33. The apparatus of claim 26, wherein said at least one of a plurality of devices that store information authenticates a source of said data packet based upon a user address in said data packet.

34. A method for managing storage, comprising:

receiving a data packet;

searching for a virtual destination address retrieved from said data packet;

reading a corresponding destination address for a particular one of at least one of a plurality of devices that store information; and

replacing in said data packet said virtual destination address with said corresponding destination address.

[図 1]

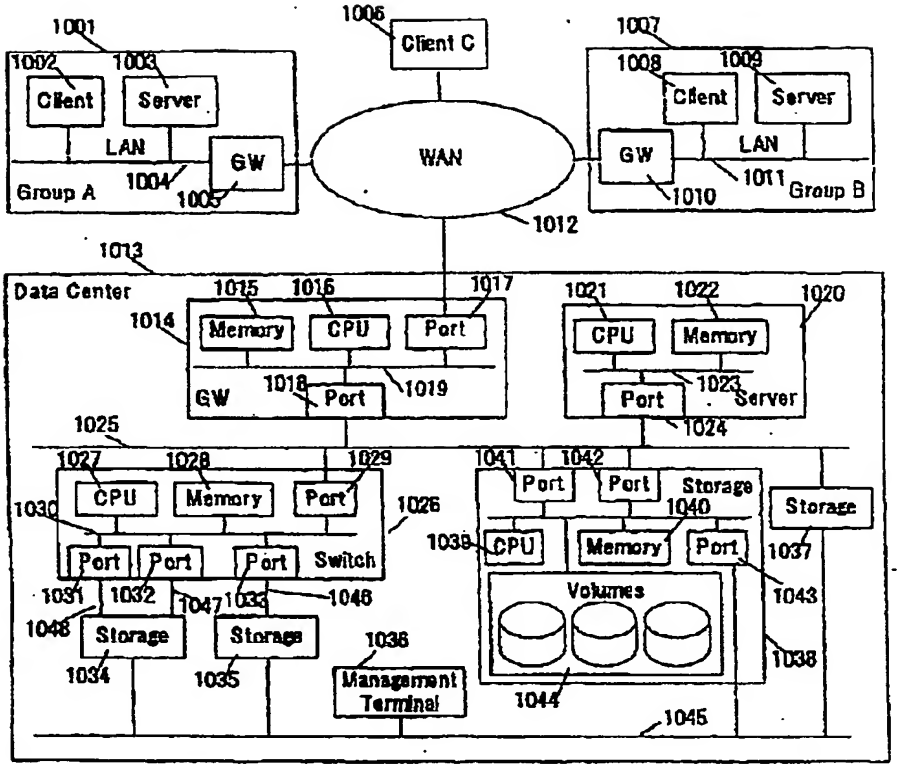


Fig. 1.

[図 2]

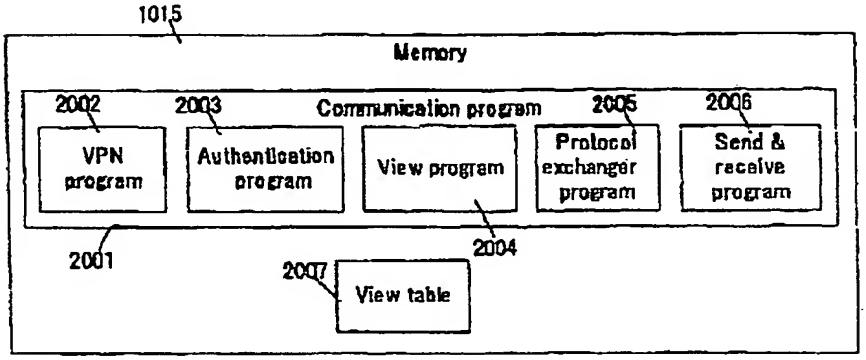


Fig. 2

【図３】

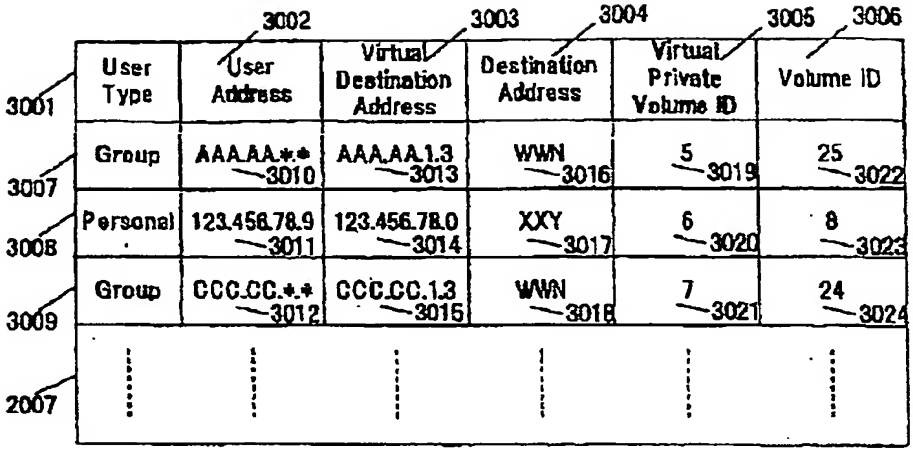

3001
3002
3003
3004
3005
3006
User Type
User Address
Virtual Destination Address
Destination Address
Virtual Private Volume ID
Volume ID
3007
Group
AAA.AA.*.*
3010
AAA.AA.1.3
3013
WWN
3016
5
3019
25
3022
3008
Personal
123.456.78.9
3011
123.456.78.0
3014
XXY
3017
6
3020
8
3023
3009
Group
CCC.CC.*.*
3012
CCC.CC.1.3
3015
WWN
3018
7
3021
24
3024
2007

Fig. 3

【図４】

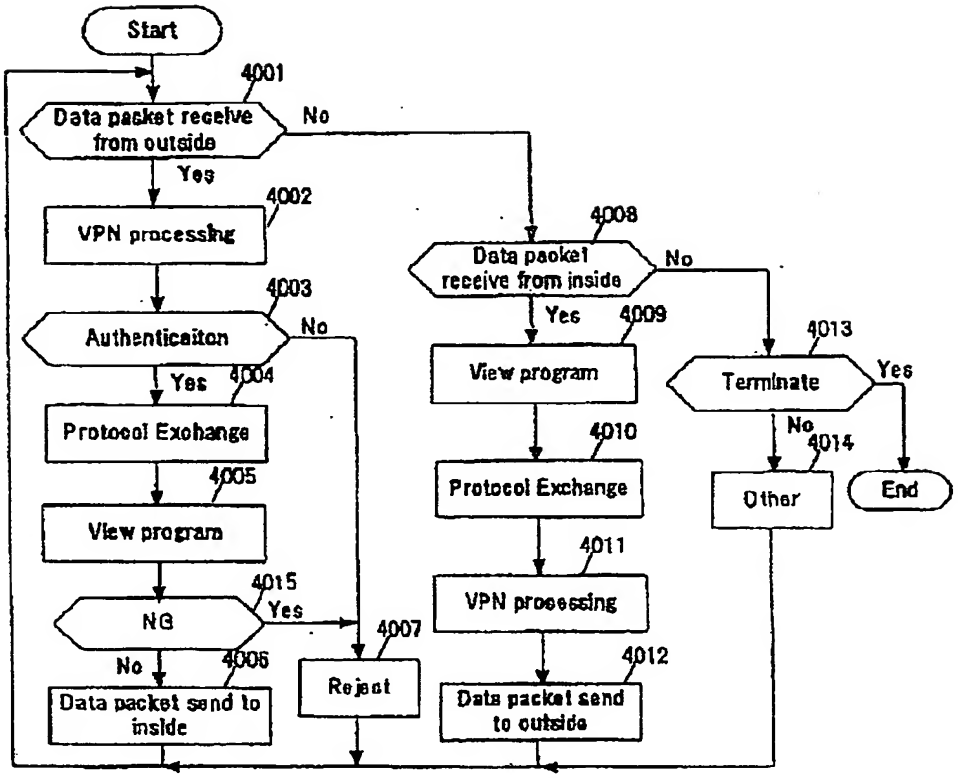

Start
4001
Data packet receive from outside
No
Yes
4002
VPN processing
4003
Authenticaiton
No
Yes
4004
Protocol Exchange
4005
View program
4015
NG
Yes
No
4006
Data packet send to inside
4007
Reject
4008
Data packet receive from inside
No
Yes
4009
View program
4010
Protocol Exchange
4011
VPN processing
4012
Data packet send to outside
4013
Terminate
Yes
No
4014
Other
End

Fig. 4

【図５】

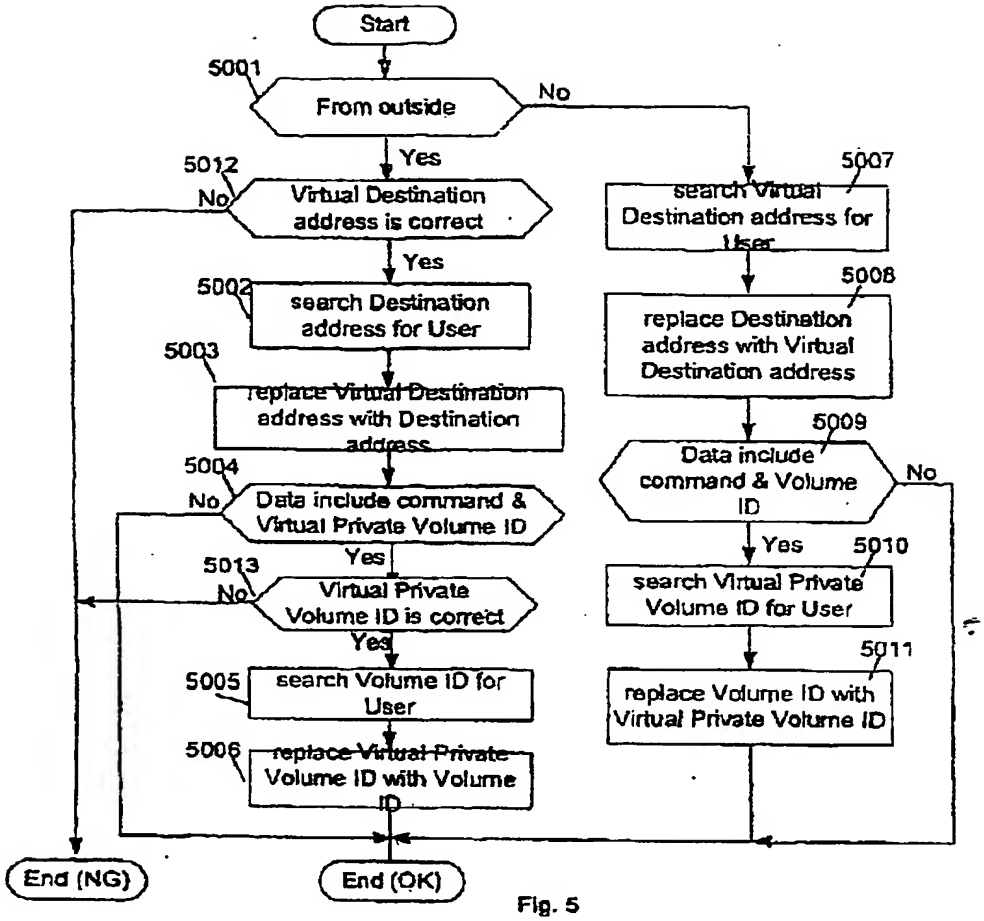

Start
5001
From outside
No
Yes
5012
No
Virtual Destination address is correct
Yes
5002
search Destination address for User
5003
replace Virtual Destination address with Destination address
5004
No
Data include command & Virtual Private Volume ID
Yes
5013
No
Virtual Private Volume ID is correct
Yes
5005
search Volume ID for User
5006
replace Virtual Private Volume ID with Volume ID
5007
search Virtual Destination address for User
5008
replace Destination address with Virtual Destination address
5009
Data include command & Volume ID
No
Yes
5010
search Virtual Private Volume ID for User
5011
replace Volume ID with Virtual Private Volume ID
End (NG)
End (OK)

Fig. 5

【図６】

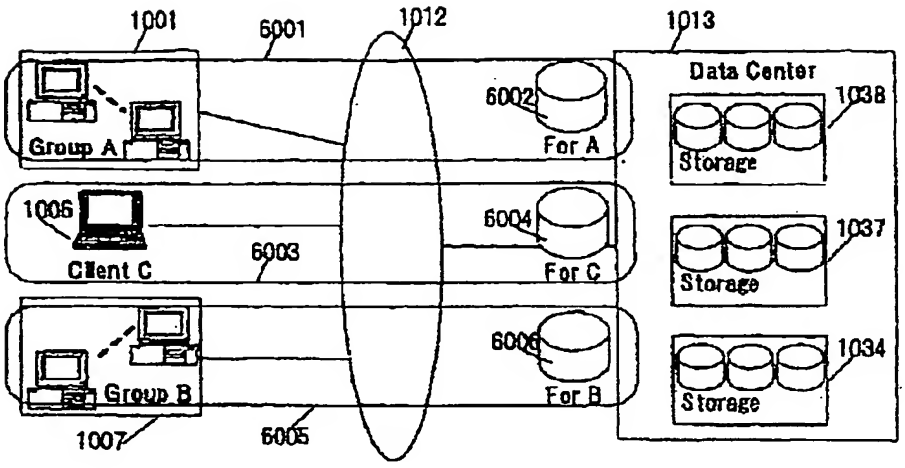


Fig. 6

【図７】

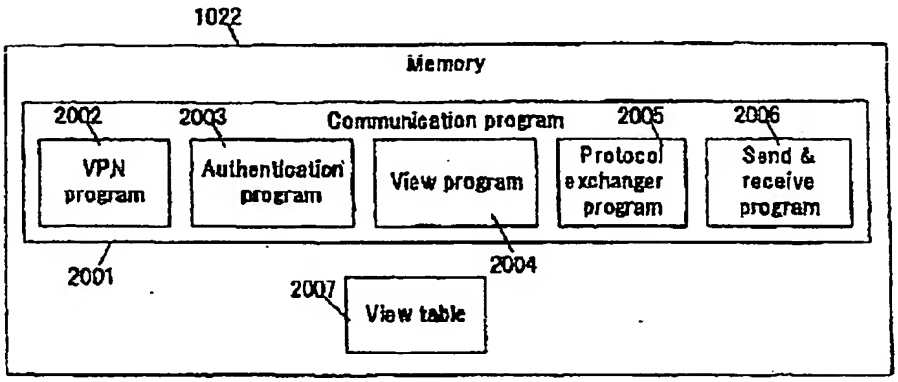


Fig. 7

【図８】

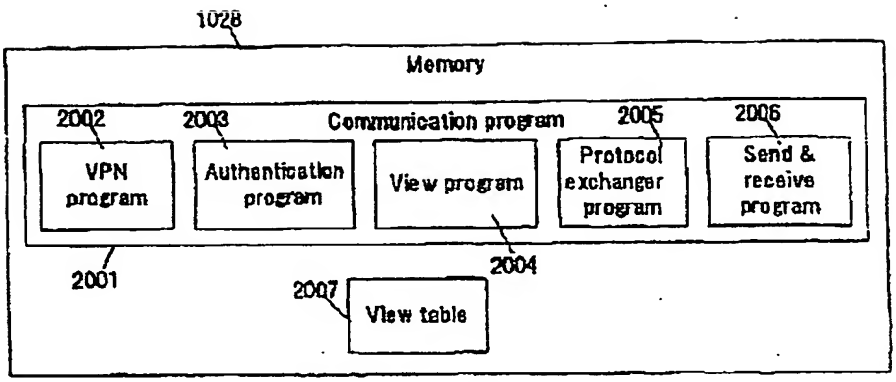


Fig. 8

【図９】

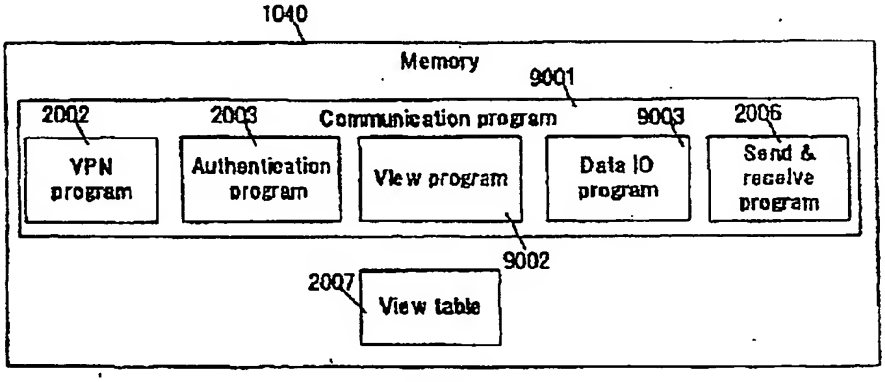


Fig. 9

【図１０】

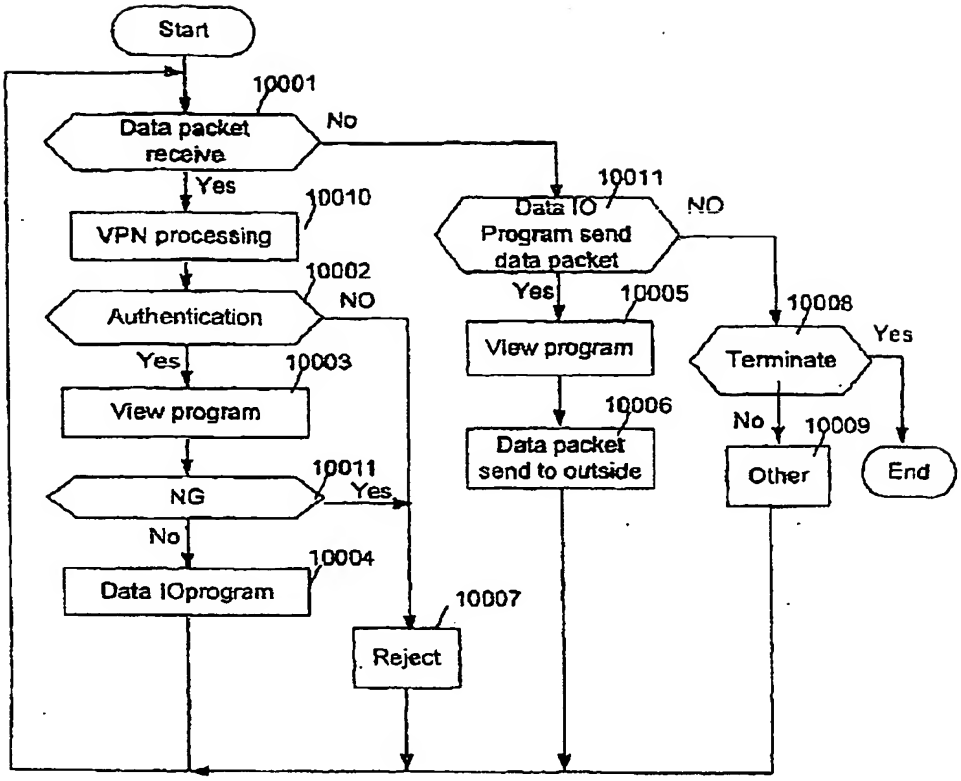

Start
10001
Data packet receive
No
Yes
10010
VPN processing
10002
Authentication
NO
Yes
10003
View program
10011
NG
Yes
No
10004
Data IOprogram
10007
Reject
10011
Data IO Program send data packet
NO
Yes
10005
View program
10006
Data packet send to outside
10008
Terminate
Yes
No
10009
Other
End

Fig. 10

[図１１]

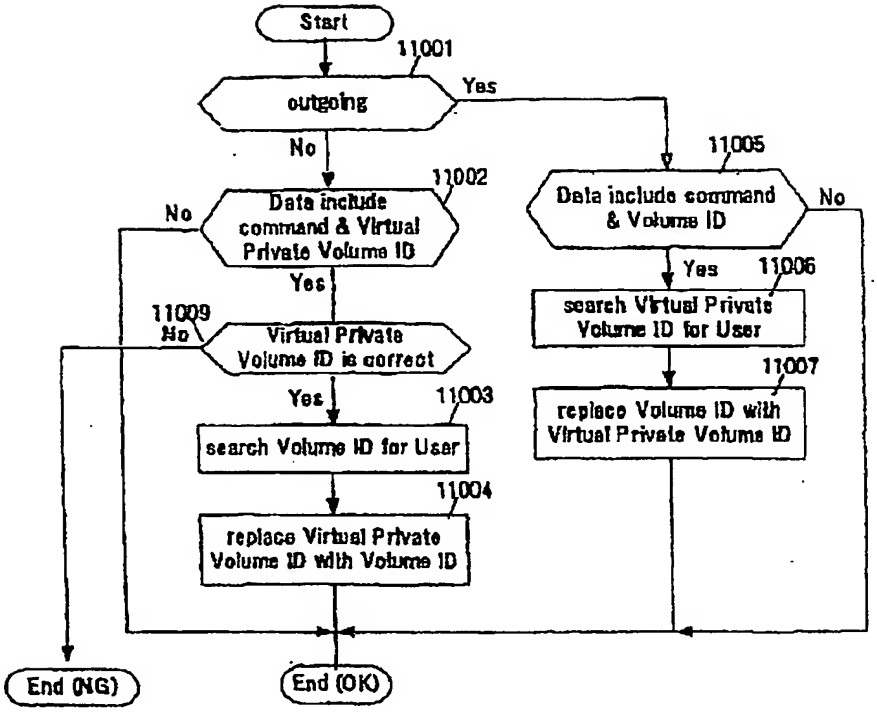

Start
11001
outgoing
Yes
No
11005
Data include command & Volume ID
No
11002
Data include command & Virtual Private Volume ID
No
Yes
Yes
11006
search Virtual Private Volume ID for User
11009
No
Virtual Private Volume ID is correct
11007
replace Volume ID with Virtual Private Volume ID
Yes
11003
search Volume ID for User
11004
replace Virtual Private Volume ID with Volume ID
End (NG)
End (OK)

Fig. 11

Virtual Private Volume Method and System

ABSTRACT OF THE DISCLOSURE

The present invention provides techniques for managing access to storage resources. In specific embodiments, storage devices provide storage resources to users using a system of virtual addresses and virtual volume identifiers. In select specific embodiments, a storage service provider (SSP) can make volumes available to a user, which may be a company, for example, in the user's network via the Internet or other kinds of network connections. In specific embodiments, the SSP and the user's data center can conceal the identity of the storage devices, volumes, and equipment of the SSP, as well as that of the user's data center in order to provide privacy to both user and storage provider.